Cloud Platform and Infrastructure Security

Cloud Platform Components

- **Network and Communication Infrastructure**
  - Network, connectivity, bandwidth, security controls etc.
- **Compute**
    - Memory, CPU, interface, Graphical Process, I/O etc
- **Management Plane**
  - Provides control of the network, communications, compute and other service elements

Shared Risk and Responsibility

- Risks will be shared between the cloud provider and the customer
- Cloud customer is ultimately responsible and legally liable for the data hosted in the Cloud
- Cloud Service provider is mostly concerned with the security and operations of its data center.

Risks in Private Cloud model

- Personnel Threats
- Natural Disasters
- External Threats
- Regulatory Noncompliance
- Malware

Risks in Public Cloud model

- Customer loses control
- Oversight
- Enforcement capabilities
- Vendor Lock-in

Controls against Vendor Lock-in

- Ensure favorable service contract
- Avoid proprietary formats
- Ensure there are no physical or technical limitations to moving
- Check for regulatory constraints

Controls against Vendor Lock-out

- Check for Provider longevity
- Core Competency
- Jurisdictional Suitability
- Supply Chain Dependencies
- Legislative Environment

Multitenant environment Risks

- Conflict of Interest
- Escalation of Privileges
- Information Bleed
- Legal Activity

IaaS Risks

- Personnel Threats
- External Threats
- Lack of Skilled workforce

PaaS Risks

- Personnel Threats
- External Threats
- Lack of Skilled workforce
- Interoperability issues
- Persistent backdoors
- Virtualization risks
- Resource Sharing

SaaS Risks

- IaaS + PaaS +
- Proprietary Formats
- Web Application Security

Virtualization Risks

- **Guest Escape:**
  - Poorly configured virtualized machine or hypervisor might allow for a user to leave the confines of their own virtualized instance
  - A user who has successfully performed guest escape might be able to access other virtualized instances on the same host
- **Host Escape**:
  - A user can not only leave their own virtualized instance, but they can also even leave the host machine, accessing other devices on the network
- Information Bleed / Side channel attack or Covert channel attack
- (Legal) Data Seizure

Cloud Threats

- Malware:
  - Less likely in SaaS
- Internal Threats:
  - Malicious or accidental activity of an authorized user
  - Applicable for all threats
- External Threats
- Man-in-the-middle Attacks / On-path Attacks
- Theft / Loss of devices

Cloud Threats

- Regulatory Violations
- Natural Disasters
- Loss of Policy control
  - Customers prefer CASB to address this
- Loss of Physical control
- Lack of Audit Access
- Contractual failure
- Escalation of Privilege

Cloud Threats Risk Mitigation

Threat	Mitigation(s)
Malware	Host / NW Anti-malware applications; Training, Continuous Monitoring and baseline configurations; Regular patches / updates
Internal Threats	Background Verification, reference confirmation, skills and knowledge testing. Mandatory vacation, recurring training, job rotation
External Threats	Hardened Physical Devices, Hypervisors, and VMs. Solid security baseline and thorough configuration / Change management. Threat Intelligence
Man-in-the-Middle	On-path attacks can be addressed by Encryption and Authentication
Social engineering	Training, spot checks and bonuses; gamification
Data Loss from Theft / Device loss	Encryption, Strict Physical access controls, no external connectivity, Comprehensive Asset inventory, remote wipe / Kill switch
Regulatory Violations	IRM, Encryption, obfuscation; strong legal knowledge

Cloud Threats Risk Mitigation

Threat	Mitigation(s)
Natural Disasters	Disaster backup, redundancy
Loss of Policy Control	CASB, Contractual terms, Audits
Loss of Physical Control	Contractual Terms, Audits
Loss of Audit Access	Third-party Audits, SOC2 reports, Contractual terms
Rouge Administrator	Privileged Access control, secure logging, locked racks, monitoring of physical access to devices, implementation of video surveillance and financial monitoring of privileged personnel
Escalation of Privilege	Extensive access control and authentication tools Skilled personnel
Contractual Failure	Full offsite backups, secured and kept by the customer or third-party vendor

Securing Communications and Infrastructure

- There are four critical concepts related to network security are:
- **Network Security Groups**
  - Virtual firewalls used in cloud environment
- **Traffic Inspection**
  - Inspection in cloud environments will be difficult compared in on-premise environment
- **Geofencing**
  - Access provisioning, triangulating access based on the geo location
- **Zero Trust**
  - Relies on identities and authorization to validate access to data

Honeypots

- A tool to distract potential attackers
- Dummy machine with fictious data seemingly valuable to entice the attackers
- Helps organization to understand the methods and motives of the attackers
- In the cloud context, setting up Honeypots will incur additional cost and hence value of a honeypot needs to be determined before building one in cloud

Identity Challenges in Cloud

- Identity Proofing, process of validating the identity to a user, is difficult if users are allowed to use public IDs for access
- Validating that users are legitimately who are supposed to use the credentials

Hardware Security Modules (HSM)

- HSM are used to generate, store and manage cryptographic keys
- They are also used to support hashing and digital signatures as well as encryption / decryption of TLS offloading and database transparent encryption

Securing Software

- Focuses on 3 areas
  - Third-party Software Management
  - Validated open-source software
  - OS Hardening, baselines, monitoring and remediation

Third-party Software Management

- When selecting a software look for
  - Fit-to-business need
  - Third-party providers practices for updates and security patching as well as their notification process
- Once the software is selected,
  - Understand the functional, configuration requirements and security implications
  - Common code elements like libraries are major concerns hence software composite analysis tools are important

Validating Open-Source Software

- Validating is very difficult because identifying a trusted source for the software and ensuring that the package is trusted is challenging
- Cryptographic checks can assist for some software packages

Hardening, Monitoring and Remediation

- OS Hardening is a very important requirement
- Baselines are a best way to hardening the operating systems.
- Baselines provides the configuration standard that meets the functional and security goals of the organization
- Baselines are the starting point in hardening

Managing Virtual Systems

- Virtualization Management tools are a very important component in protecting the virtual infrastructure
- It can help map storage, support improved networking, improve experience and functionality for virtualized OS
- Configuration of host / guest System backup and restore functionalities

Securing the Management Plane

- There are 3 critical elements in Management Plane security
  - **Scheduling**: Starting or stopping resources at a planned time or due to events. This is a key element in cost control
  - **Orchestration**: Automating process and workloads
  - **Maintenance**: managing, upgrading ephemeral, code-defined systems as they are added and removed

Management Plane Security best practices

- Muti-factor authentication for all accounts
- Secrets management training
- Provisioning practices ensuring rights are provisioned seamlessly
- Least privilege approach for rights and roles
- Monitoring and alerting
- Limitation of root account
- Use of security groups and other access control mechanisms

SOC Audits

SOC Type	Description
SOC 1	Auditing the financial reporting instruments of an organization Focused by financial auditors of user organization
SOC 2	Audit on organization’s security, availability, processing integrity, confidentiality and privacy Used by Security Practioners Detailed reports not shared publicly
SOC 3	Summary reports that are shared publicly They contain no actual data instead just an assertion that they organization has passed the assessment

Assessment	Description
Type 1	Focuses on Design efficiency of the controls
Type 2	Focuses on operating efficiency of the controls Need atleast 6 months of past data to validate control efficacy

All the best