CLOUD SECURITY: SOLUTIONS

SAMITHA SOMATHILAKA

Department of Computing & Mathematics, WIT

ADVANTAGES OF CLOUD SECURITY

CENTRALIZED SECURITY

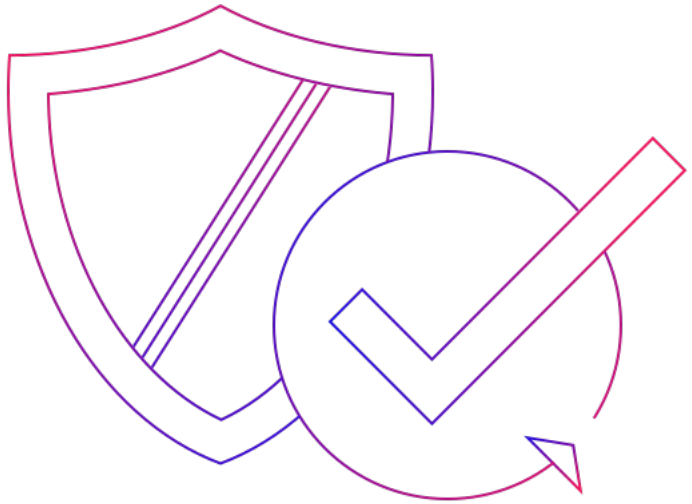
- Just as cloud computing centralizes applications and data, cloud security centralizes protection.
  - Cloud-based business networks consist of numerous devices and endpoints that can be difficult to manage when dealing with ideas such as **BYOD**.
  - Managing these entities centrally enhances traffic analysis and web filtering, streamlines the monitoring of network events and results in fewer software and policy updates.
- Disaster recovery plans can also be implemented and actioned easily when they are managed in one place.

REDUCED COSTS

- One of the benefits of utilizing cloud storage and security is that it eliminates the need to invest in dedicated hardware.
- Not only does this reduce capital expenditure, but it also reduces administrative overheads.
- Where once IT teams were firefighting security issues reactively, cloud security delivers proactive security features that offer protection 24/7 with little or no human intervention.

RELIABILITY

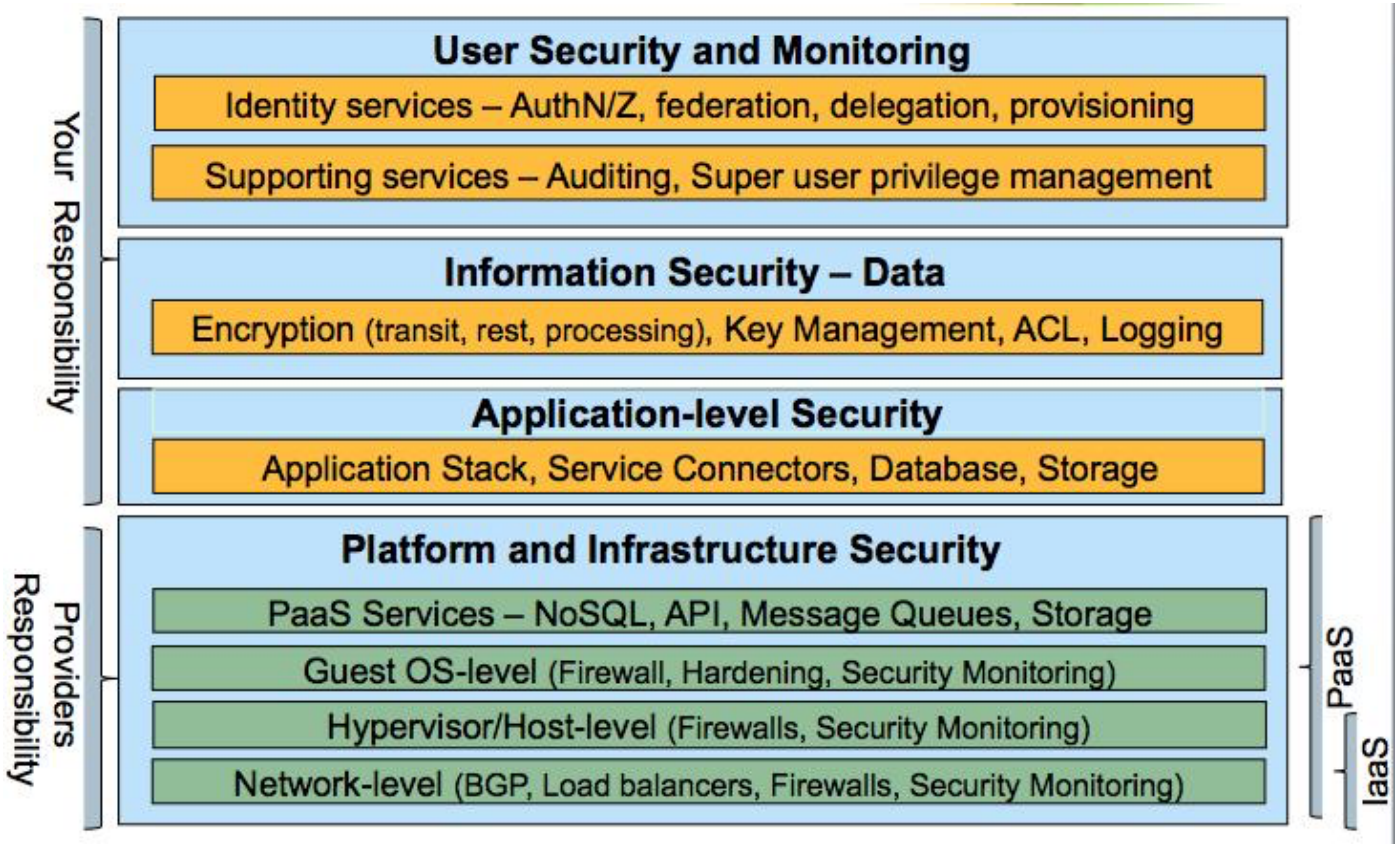
- Cloud computing services offer the ultimate in dependability.
- With the right cloud security measures in place, users can safely access data and applications within the cloud no matter where they are or what device they are using.



SEGREGATION OF RESPONSIBILITY

- By definition, cloud security responsibilities in a public cloud are shared between the cloud customer (your enterprise) and the cloud service provider whereas in a private cloud, the customer is managing all aspects of the cloud platform.
- Cloud service providers are responsible for securing the shared infrastructure including routers, switches, load balancers, firewalls, hypervisors, storage networks, management consoles, DNS, directory services and cloud API.

SEGREGATION OF RESPONSIBILITY



SOLUTIONS

POSSIBLE SOLUTIONS

- Minimize Lack of Trust
  - Policies
  - Certification
- Minimize Loss of Control
  - Monitoring
  - Utilizing different clouds
  - Access control management

MINIMIZE LACK OF TRUST: POLICIES

- Consumers have specific security needs but don’t have a say-so in how they are handled
  - What is the provider doing for me?
  - Agreed upon and upheld by both parties
  - Can be used in a intra-cloud environment to realize overarching security posture

MINIMIZE LACK OF TRUST: CERTIFICATION

- Certification
  - Some form of reputable, independent, comparable assessment and description of security features and assurance
  - Sarbanes-Oxley, DIACAP, DISTCAP, etc (are they sufficient for a cloud environment?)
- Risk assessment
  - Performed by certified third parties
  - Provides consumers with additional assurance

MINIMIZE LOSS OF CONTROL: MONITORING

- Cloud consumer needs situational awareness for critical applications
  - When underlying components fail
  - What recovery measures can be taken (by provider and consumer)

- Requires an application-specific run-time monitoring and management tool for the consumer
  - The cloud consumer and cloud provider have different views of the system
  - Enable both the provider and tenants to monitor the components in the cloud that are under their control

MINIMIZE LOSS OF CONTROL: UTILIZE DIFFERENT CLOUDS

- The concept of ‘Don’t put all your eggs in one basket’
  - Consumer may use services from different clouds through an intra-cloud or multi-cloud architecture
  - Propose a multi-cloud or intra-cloud architecture in which consumers
    - Spread the risk
    - Increase redundancy (per-task or per-application)
      - Increase chance of mission completion for critical applications

MINIMIZE LOSS OF CONTROL: UTILIZE DIFFERENT CLOUDS

- Possible issues to consider:
  - Policy incompatibility (combined, what is the overarching policy?)
  - Maximized cost
  - Incompatibility with protocols

MINIMIZE LOSS OF CONTROL: ACCESS CONTROL

- Regardless of deployment model, provider needs to manage the user authentication and access control procedures (to the cloud)
  - Federated Identity Management: access control management burden still lies with the provider
  - Requires user to place a large amount of trust on the provider in terms of security, management, and maintenance of access control policies. This can be burdensome when numerous users from different organizations with different access control policies, are involved

MINIMIZE LOSS OF CONTROL: ACCESS CONTROL (CONT.)

- Consumer-managed access control
  - Consumer retains decision-making process to retain some control, requiring less trust of the provider
  - It also needs to be able to guarantee that the provider will uphold the consumer-side's access decisions.

MINIMIZE LOSS OF CONTROL: IDM

- **Enhanced Network Abilities:** Identity management (IDM) makes it simple in sharing the network capabilities with a complete grid of users who were connected with it.
- **Provides a secure collaboration:** SaaS protocol is designed and utilized as a hub for connecting with all virtual networks of suppliers, distributors, and trading partners.
- **Centralized Management System:** Business users can be able to manage all services and programs at one place with the cloud-based services. Identity management can be done with one click on a single dashboard.