

el
by E E

Submission date: 14-May-2022 06:29PM (UTC+0530)

Submission ID: 1836124136

File name: Cloud.docx (146.77K)

Word count: 961

Character count: 5375

Table of Contents

Challenges that Musica can face while migrating to cloud computing	1
Incompatibility	1
Financial Cost	1
Skill Shortage.....	2
Legacy Apps.....	3
Downtime.....	3
Data security	3
Data sovereignty regulations	3
Cloud security	3

Challenges that Musica can face while migrating to cloud computing

Incompatibility

Most firms suffer a gap between what they have on-premises and how the service they are going to buy is used during their migration to the public cloud. When companies like Musica go to the cloud, they may suffer a gap between their on-premises architecture and the cloud infrastructure.

Cloud providers have attempted to provide such connectors, but the problem is that most companies' underlying technology is different. Only a few businesses go completely cloud, but the majority prefer to use a hybrid model. These hybrid models cause interoperability issues with current cloud providers. (Ghanam, n.d.)

Financial Cost

Musica must rewrite its application architecture to be compliant with the cloud provider to go to the cloud.

To move and sustain successfully, the organization must also invest in people and the necessary tools. Although the cost of maintenance and administration will drop in the future, the cost of this migration is quite high.

Skill Shortage

The advantages of cloud computing are undeniable, but the complexity of the migration prevents businesses from doing so. Finding qualified employees with the right skill set to efficiently migrate to the cloud is one of the biggest obstacles to migration.

Because most businesses are attempting to migrate to the cloud, demand for cloud expertise is exceeding supply. As Cloud Computing is a relatively newer technology finding, hiring and retaining employees with the necessary skills is a very difficult task.

According to a McAfee analysis, the talent gap in the existing IT industry, which lacks in the cyber security arena, accounts for 40% of the slow migration to the cloud.



Figure 1 Cloud Challenges for Musica

Legacy Apps

Although Musica's codebase is rapidly evolving, it still contains a few legacy apps that cannot be migrated to a virtual cloud environment. In these situations, the organization must rewrite the legacy apps using recent technology. If these systems and apps are critical to the business, moving to the cloud may be extremely difficult. (Logesswari Srinivasan, n.d.)

Downtime

In today's world, disruption or downtime is unavoidable. By putting IT infrastructure in the cloud, a corporation must rely on the Cloud service provider to ensure that service is not interrupted. If a problem or disruption occurs, the Company needs to wait for service provider updates and fixes.

And the company may not have any control over the downtime that occurs.

Data security

Although Cloud service providers take care of their cloud platform and data's security, they are not responsible for Musica's applications, servers, and data. Service providers are not liable in case of a Data breach

Musica must encrypt and safeguard essential data on its own, as well as invest in a suite of products from service providers such as antivirus, secure online gateways, and malware detectors, all of which add to the financial burden. (Saxena, n.d.)

Data sovereignty regulations

Data sovereignty laws are one of the most typical challenges Musica may encounter. Some nations impose restrictions on corporations' ability to keep sensitive data in data centers located in other countries. There are policies specific to government departments that obstruct migration plans. (Huey, n.d.)

Cloud security

Cyberattacks on cloud-based applications, data, and infrastructure are a serious concern. Cloud computing requires some technology, policies, and controls to be secure. Service providers and consumers share responsibilities for cloud security.

Data on the cloud should be encrypted, and proxies and brokerage services should be used to prevent unauthorized access. (Tauro, n.d.)

Each cloud service model has a varied level of cyber security, such as IaaS, PaaS, and SaaS. At various levels of service, these models require customers to be responsible for security.

Because cloud security is a shared responsibility, many service models have their distinctions between customer and service provider responsibilities. (Tushar Parmanand Budhwani, n.d.)

To address the difficulties of boundaries, the Cloud Security Alliance (CSA) was established, which specifies the boundaries of various service models and how they relate to one another. The CSA stack model is depicted in the diagram below:

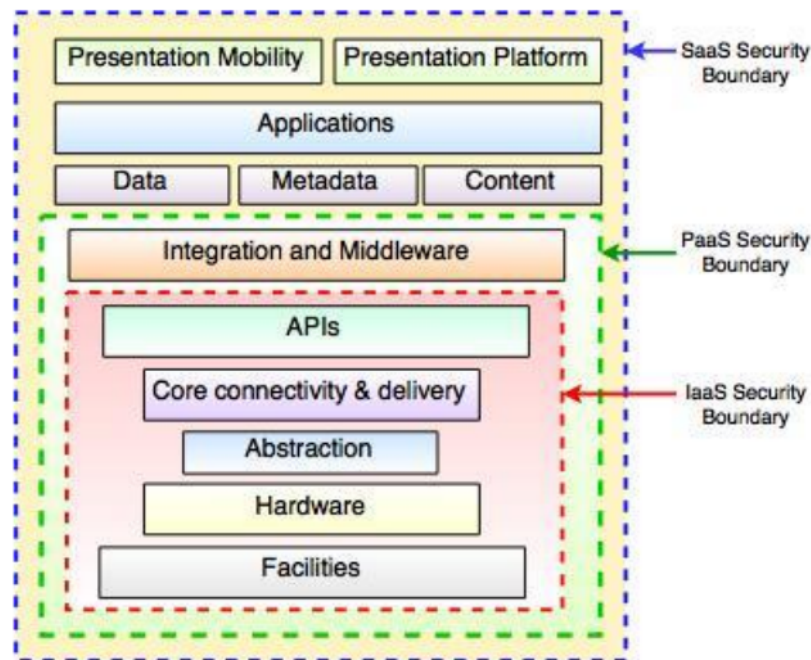


Figure 2 CSA Stack model (Tauro, n.d.)

IaaS offers the least amount of integrated functionality and security, whereas SaaS offers the greatest. The security boundaries between the cloud service provider's and the customer's duties are defined by this model. Any security mechanism that extends outside the security barrier must be implemented into the system and maintained by the customer.

Although each service architecture has its security mechanisms, the security requirements differ depending on whether the services are in a private, public, hybrid, or community cloud.

Musica must include Network Segmentation, Intrusion Detection Systems, and Virtual Firewalls in their web-based application to safeguard it from malicious malware. They must also incorporate Intrusion Prevention Systems (IPS) such as (IDS and IPS). Virtual routers are also required by the company.

In addition to this high-end solution, Musica should log IP addresses and whitelist and blacklist APIs if the service is accessible using a web-based API.

In the event of a disaster or failure, the company must also assure for data recovery.

References

Ghanam, Y., n.d. Emerging Issues & Challenges in Cloud Computing—A Hybrid Approach. *Journal of Software Engineering and Applications*.

Huey, E., n.d. Cloud Computing-Challenges and Benefits. *International Journal of Computer Trends and Technology*.

Logesswari Srinivasan, S. J., n.d. A study on cloud computing challenges and its mitigations. *Materials Today*.

Saxena, v., n.d. Cloud computing challenges and implementations. *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*.

Tauro, J. S., n.d. Overview of Cloud Security.

Tushar Parmanand Budhwani, P. T., n.d. An Analysis of Cloud Security.

ORIGINALITY REPORT

0%

SIMILARITY INDEX

0%

INTERNET SOURCES

0%

PUBLICATIONS

0%

STUDENT PAPERS

PRIMARY SOURCES

Exclude quotes On

Exclude bibliography On

Exclude matches Off