Cybersecurity Proposal

Prasanthi Desiraju, Vittorio Pepe, and Will Shin

MSDS 485 Data Governance, Ethics & Law

May 22, 2021

INTRODUCTION

In this study, we propose a cloud service provider to manage your company application from a cybersecurity standpoint. Other factors should be considered before making a final decision. The most relevant is the main operative system, database system, and technical specs of the applications that need to be migrated to the cloud. While all the providers considered offer some form of multiplatform approach, some are better than others on specific platforms.

The vendors considered in this study are Oracle Cloud Infrastructure (OCI), Amazon Web Services (AWS), and Microsoft Azure. We propose implementing OCI because although it is a relatively new player in the market, its platform has been developed to address cybersecurity issues from the initial phases of the system design and build upon the experience made by the other major players on the market.

THE COMPANY

Oracle Corporation is an American multinational computer technology corporation based in Austin Tx, that offers a wide range of software products. The company was founded in 1997, and it became renewed for its database software. Since the acquisition of Peoplesoft in 2005 and SunMicrosystem in 2010, it progressively moved into the application solution business (ERP, CRM, etc.) and in 2016 into the cloud computing arena [1]. It is ranked in the Forbes global report of 2020 as the second-largest software provider by revenue and market capitalization, after Microsoft [2][3].

PRODUCT FUNCTIONALITIES

The OCI is the cloud computing service offered by Oracle, and it provides hardware hosting, storage, network, and application and services. It is delivered in four main offerings as [4]:

1. Infrastructure as service (Oracle IaaS)
2. Platform as Service: Oracle PaaS
3. Software as Service (Oracle SaaS)
4. Data as Service (Oracle DaaS)

Oracle has a dedicated security and compliance solution that comprises the following functionalities [5]:

Identity and Access Management: the solution is based on the database management type of security and allows the definition of users and groups, with the permission to access company resources is granted at the group level. This reduces the amount of setup time and gives better visibility on the permissions granted.

Data Safe: it is included with every Oracle Cloud database, and it is also available for Oracle databases that are not hosted in the cloud. It provides a single console to perform security assessments, user risk assessments, activity auditing, sensitive data discovery, and data masking.

CASB Cloud Service: Oracle Cloud Security Broker (CASB) is a security automation tool that allows detecting threats on the full cloud architecture. It can detect anomalies and fraud using advanced behavioral analysis. This tool offers reporting capabilities that help monitor regulatory compliance across the full cloud stack.

Vault: Oracle Cloud Infrastructure Vault is a user key management service that allows the centralized management of encryption keys. It is worth noticing that all relational databases (both Oracle and Microsoft SQL) are encrypted by default.

Web Application Firewall: it is a cloud-based service that helps to protect the company's web-facing application from malicious and unwanted internet traffic. It relies on threat intelligence and consistent rules enforcement to protect against cybersecurity attacks.

Cloud Guard: this tool detects misconfigured resources and insecure activities, allowing the resolution of cloud security issues. It provides a suite of out-the-box security recipes and settings that automatically fix security risks and inconsistencies.

Security Zone: this tool automatically sets up and enforces security policies on the various company compartments in the Oracle cloud. It is based on best practices and comes with a library of predefined policies that help a quick setup of the company's security.

Identity Cloud Service: it is a centralized tool that allows the management of user access, both for internal and external users. It provides a consistent way across all devices, locations, and services. It also provides the most modern capabilities as adaptive authentication and single sign-on to help reduce the operational complexity for the users without compromising on security.

The above mentioned functionalities that come bundled with an existing cloud service provider appears to be a sustainable option rather than having an inhouse development to achieve the same functionalities. These responsibilities are often time consuming and pull away from the business critical tasks and hence we recommend to go with an existing CSP. In addition, Oracle also supports four deployment options, the public cloud, private cloud, hybrid cloud and community cloud. A private cloud will be better suited for the enterprise if the firm insists on creating the infrastructure, the security, the service offerings, the service level objectives. It helps utilize all the services of cloud service providers and yet have it exclusively under the firm’s control.[12]. These deployments are available in the following

three CSP's and the kind of deployment can be decided later, that fits the firm's policies in a better way, once a CSP is established.

COMPARISON

When comparing the capabilities between these three cloud service infrastructures, Oracle boasts where they come out ahead.[6]

Capabilities and Evidence	Oracle Cloud Infrastructure	Microsoft Azure	Amazon Web Services
Native VMware-based cloud environment that gives the customer complete full administrative control.	X		
End-to-end Service Level Agreement (SLA) ability to manage, monitor, and modify cloud resources.	X		

What is also unique about Azure and AWS, however, is that both of these two cloud services can host Oracle database.[7] Some advantages that organizations may consider the advantages include Azure offering FIPS-140-2-compliant data encryption at rest, role-based access controls (RBACs), active directory authentication, and enhanced data securities by presenting mount points within a virtual private cloud rather than a public IP address.[7] In contrast, AWS can host an Oracle database on either EC2 instances or AWS Relational Database Service (RDS). The advantage to this architecture is that each EC2 can offer different configurations and resources, but at the cost of performance and reliability. While Oracle within Azure provides more control than Oracle within AWS, Oracle within AWS provides greater simplicity.[8]

RECOMMENDATION

Each cloud service infrastructure vendor has their advantages over the other. No one clear winner stands out by any wide margin. However, we recommend Oracle Cloud Infrastructure. AWS, who provides the simplest control and least administrative control to users, have deflected responsibility of data breaches in the past to their client (the owners of the data). [9] Azure also did likewise in 2019.[10]

One of the marks of great leadership is that they take responsibility.[11] It is worth noting that almost all cybersecurity companies will boast and advertise themselves as leaders of cybersecurity, but then when a cybersecurity breach occurs, they will exhibit no leadership mark of taking responsibility. Instead, they quickly cast the blaming finger at the owners of the data - their customer. Oracle, however, believes in what they call "shared responsibility." On one hand, unlike AWS and Azure, they will accept responsibility but, on the other hand, not all of it. They are willing to share the burden of responsibility should a breach occur with their cybersecurity cloud infrastructure.[12]

REFERENCES

[1] 2021. *Oracle*. Accessed May 23. https://www.oracle.com/corporate/.

[2]"The Global 2000 2021." 2021. *Forbes*. Forbes Magazine. Accessed May 23. https://www.forbes.com/lists/global2000/#66bf866f5ac0.

[3]"List of the Largest Software Companies." 2021. *Wikipedia*. Wikimedia Foundation. May 21. https://en.wikipedia.org/wiki/List_of_the_largest_software_companies.

[4] Chand, Mahesh. 2021. "Top 10 Cloud Service Providers In 2021." *C# Corner*. Accessed May 23. https://www.c-sharpcorner.com/article/top-10-cloud-service-providers/.

[5]"Integrated Cloud Applications and Platform Services." 2021. *Oracle*. Accessed May 23. https://www.oracle.com/product-navigator/?product=mpd-cld-infra%3Asecurity-id-compliance%3Aidentity-cloud-service.

[6]“Migration to the Cloud Made Simple.” 2021. *Oracle*. Accessed May 23. https://www.oracle.com/cloud/.

[7] Limor Maayan. 2020. “Oracle Database in the Cloud: Azure vs AWS vs Oracle.” *Compare the Cloud*. June 3. https://www.comparethecloud.net/articles/oracle-database-in-the-cloud-azure-vs-aws-vs-oracle/.

[8] Prabu Arjunan, Solution Architect. 2019. “A Reference Architecture for Deploying Oracle Databases in the Cloud.” *NetApp Cloud Solutions Homepage*. Netapp. August 28. https://cloud.netapp.com/blog/ma-anf-blg-deploy-oracle-databases.

[9] Graham, Jefferson. 2019. “Capital One Data Breach: Amazon Web Services Is Backbone for Netflix, NASA and Others.” *USA Today*. Gannett Satellite Information Network. July 30. https://www.usatoday.com/story/tech/talkingtech/2019/07/30/amazon-aws-unit-says-its-not-responsible-capital-one-data-breach/1868862001/.

[10] Simon, Michael. 2019. “Mystery Data Breach Reportedly Exposes 80 Million Names, Addresses, and Income Info in U.S.” *PCWorld*. PCWorld. April 29. https://www.pcworld.com/article/3391916/mystery-data-breach-reportedly-exposes-80-million-names-addresses-and-income-info.html.

[11]Zenger, Jack. 2015. “Taking Responsibility Is The Highest Mark Of Great Leaders.” *Forbes*. Forbes Magazine. July 16. https://www.forbes.com/sites/jackzenger/2015/07/16/taking-responsibility-is-the-highest-mark-of-great-leaders/?sh=3c83560048f2.

[12]Cloud Threat and Security Report https://www.oracle.com/a/ocom/docs/cloud/oracle-cloud-threat-report-2020.pdf