ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 2, pp: (50-51), Month: April - June 2021, Available at: www.researchpublish.com

PROTECT SENSITIVE DATA IN THE CLOUD

Rafiq Ajmal Khurshid [1]

[1,2]Affiliation None

[1,2]Saudi Aramco, Dhahran, Saudi Arabia

Abstract: **More and more organizations embarking on the digital transformation journey to move business-critical applications to the clouds. The Internet of things (IoT) is linking people, devices, and cloud data storage services at a rapid pace. The top cloud security challenges, to be faced by organizations, are data loss/leakage and data privacy/confidentiality. This article identifies challenges faced by organizations with the adaption of cloud services and applications. Furthermore, it recommends a solution that has become a critical element of enterprise cloud security strategies.**

Keywords: **Cloud Access Security Broker, CASB, Data Insight & Protection, Data Loss Prevention, Data Leakage Prevention.**

I. INTRODUCTION

The use of cloud computing is at an unprecedented rate, with enterprise applications migrating to the public cloud and organizations becoming more cloud-native in their deployments. Adoption of cloud products and services are at a significantly increased rate creating a significant risk to the company's data, the most valuable asset of your company. With the increased adaption of the Internet of Things (IoT) and workloads migrating from on-premises to the cloud, the data security risk is becoming more alarming. Gartner predicted that more than 15 billion IoT devices will be connected to the enterprise infrastructure by 2029. This problem gets more complicated with the rise in the trend toward Bring-Your-Own-Devices (BYOD). Organizations are overwhelmed with these challenges while we didn't even discuss compliance requirements. Due to these reasons, more and more organizations are looking for the protection of their data from both outside threats as well as individuals within an organization that may compromise the data. This is especially true for organizations looking to embrace online collaboration solutions while working remotely, or that operate in highly regulated industries such as financial services, governments, healthcare, and require the highest level of control and security for their sensitive data. As a result, IT organizations are struggling to maintain visibility and accountability. Due to these reasons, Cloud Access Security Broker (CASB) is now part of the enterprise security strategy to provide Visibility, Threat Protection, Compliance, and Data Security solution.

II. DETAILED DESCRIPTION

Cloud security concerns remain high as the adoption of public clouds continues to surge. Cloud providers are offering robust security measures but customers are ultimately responsible to secure their data in the cloud. To protect data in the cloud, we need to implement Cloud Access Security Broker (CASB) solution. CASB is a technology that has resulted from the need to secure cloud services and is required to address security gaps in an organization's use of cloud services. Deploying the CASB will allow organizations to apply their security policies beyond their site to third-party software and storage.

National Cybersecurity Authority "NCA" of the Kingdom of Saudi Arabia has developed the Critical Systems Cybersecurity Controls (CSCC-1: 2019), one of the clouds hosting control (# 2-6-1-3) requests to protect classified data of critical systems using data leakage prevention (DLP) techniques. Before taking a deep dive, let's define CASB and

DLP. CASB is a security layer between users and cloud systems to help organizations manage data residing in the cloud and provide visibility and control of the cloud service. On the other hand, DLP is a set of tools and processes to enable organizations to protect sensitive data by monitoring, detecting, and blocking sensitive data while in-use, in-motion, and at-rest. Due to the potential for data leakage in the cloud, the implementation of CASB is required to protect data that has gone beyond the reach of on-premises tools. Now let's take a deeper dive into CASB and review the four (4) pillars of CASBs as defined by Gartner.

Visibility: Organizations must have full visibility on how and where sensitive data reside. With the adoption of the public cloud, sensitive data has moved from behind the enterprise firewall to the cloud. CASB solution will provide visibility on Shadow IT, also known as unsanctioned solutions. Organizations will have visibility into users, data, access, and location. Furthermore, cloud usage will be classified according to risk to help organizations to accept the risk by doing nothing or take actions such as Block.

Data Security: CASB solution will act as a safety link between your organization and the cloud service provider. Using the CASB solution, organizations will be able to enforce a data-centric policy to prevent unwanted activity based on data classification, data discovery, and user activity. CASB DLP operates natively and in conjunction with enterprise DLP products via Internet Content Adaptation Protocol (ICAP) or REST API integration.

Threat Protection: CASB solution will prevent unwanted devices and users from accessing cloud services by providing Adaptive Access Controls (AACs). It will provide the ability to identify access from suspicious hosts, devices, locations, and more. CASB solution capitalizes on User Entity Behavior Analytical (UEBA) tool to detect Insider Threats, Compromised Accounts, and Potential Exfiltration.

Compliance: CASB solution is equipped with classification functionality for data passing through the CASB, which can help to comply with laws and regulations. Furthermore, CASB can enforce DLP policies against existing data in a cloud service and new files as they are uploaded.

III. CONCLUSION

The reality on the ground is that data and users are moving off the network and moving to cloud applications and services whereas legacy security technologies are obsolete and unable to protect data in the cloud, which is the most important asset of any organization. Organizations are looking for a total cloud security solution to strengthen security, protect their sensitive data and reduce risk. CASB is a solution that will address these concerns and provide you granular approach to visibility into user activity and cloud usages, making compliance, threat Protection, Compliance, and Data Security.

REFERENCES

[1] Magic Quadrant for Cloud Access Security Brokers, Gartner, Published 22 October 2019, ID G00377508, www.gartner.com

[2] 2020 Cloud Security Report, Check Point Software Technologies Ltd., https://www.rmol.cz/sites/default/files/prilohy/2020-cloud-security-report.pdf

[3] Critical Systems Cybersecurity Controls (CSCC) https://nca.gov.sa/en/pages/cscc.html