Cloud Migration Security Risks and Solutions: A Comprehensive Overview

Prepared by

Jason Basore

Sean Berlin

Liam Daly

Scott Stahmer

April 10, 2023

Executive Summary

The purpose of this white paper is to provide an in-depth analysis of the security risks that companies face when migrating to cloud services and to offer effective solutions for mitigating these risks. Cloud migration presents a unique set of security risks for companies, including malware and viruses, insider threats, DDoS attacks, and a lack of visibility and control. These risks can lead to significant financial losses, damage to reputation, and legal liabilities. To address these risks and safeguard against potential security breaches, companies can implement a number of solutions, including the use of encryption, strong access policies, regular security testing, and clear communication between both parties. Encryption can be used to protect sensitive data during transmission and storage. Strong access policies and controls can be utilized to limit access to sensitive data. Regularly testing the security framework allows for vulnerabilities to be identified and addressed promptly. Keeping lines of communication open and transparent between the two parties will help to ensure that all security risks are quickly identified and fixed. Through our analysis of current research and industry best practices, we have identified the key security risks that companies face when migrating to the cloud, as well as effective solutions for mitigating these risks. It is critical for companies to understand these risks and take proactive steps to secure their data and systems during cloud migration.

Articulation of Problem

Malware and Viruses

There are a lot of security risks involved with transferring to and using a cloud service system. One of these risks is malware and viruses. Malware and viruses can leak, delete, or alter important data. Ransomware holds data hostage via encryption, making the victim unable to access it, until they pay a ransom. However, paying the ransom will not always ensure access to the user's data. An example of ransomware is Lumen Technologies, a telecommunications company. On March 27th, 2023, they reported that they faced two cyber security incidents. One incident managed to implement criminal ransomware into the servers while the other gained access to some of its internal information technology systems (Lahiri). Fileless malware makes its changes to the files themselves, not installing anything at first. The operating system/ security, however, miss the changes and still thinks the files are legitimate. In January and February of 2023, a fileless malware called Gootloader was used in one of the two separate campaigns that also used another of an unspecified type named SocGholish/FakeUpdates, to target six law firms (Arghire). "GootLoader is a downloader that was first identified in late 2020.[2] It has since been used to deliver a wide range of secondary payloads, such as Cobalt Strike and ransomware. The malware employs search engine optimization (SEO) poisoning to funnel victims searching for business-related documents toward drive-by download sites that drop the JavaScript malware (Hall). " "Spyware collects information about users' activities without their knowledge or consent. This can include passwords, pins, payment information, and unstructured messages" ("12 types of malware + examples that you should know"). Researchers from Google's Threat Analysis Group (TAG) have discovered two separate, highly-targeted campaigns that use various, unpatched zero-day exploits against users of both iPhone and Android smartphones to deploy spyware.

The discoveries — revealed in a blog post on March 29 — are the result of active tracking that Google TAG does of commercial spyware vendors, with more than 30 of them currently on the radar screen, the researchers said. These vendors sell exploits or surveillance capabilities to state-sponsored threat actors, thus "enabling the proliferation of dangerous hacking tools, arming governments that would not be able to develop these capabilities in-house," the researchers wrote. These are often used to target dissidents, journalists, human rights workers, and opposition-party politicians in potentially life-threatening ways, they noted (Montalbano). With this in mind, moving a large chunk of data to the cloud can make it a huge target for hackers.

Insider Threats

For businesses moving to the cloud, insider threats are a major concern. Insider threats are defined as malicious or unintentional actions that can jeopardize the confidentiality, integrity, or accessibility of data and systems by staff members, partners, or contractors of an organization. When moving to the cloud, businesses should be aware of insider threats such as data exfiltration, credential fraud, and malicious insiders. Data exfiltration is the unauthorized data transfer from an organization's network to an external destination. It can happen by emailing sensitive data to personal accounts, uploading files to unauthorized cloud accounts, or using USB drives to copy files from the organization's network. Data exfiltration is a significant issue in the context of cloud migration because sensitive data is being transferred from an organization's on-premises infrastructure to cloud services that are managed by third parties. When employees are granted access to cloud services that contain sensitive data, the risk of data exfiltration increases, especially if their access rights are not correctly restricted or monitored. Data theft can have serious consequences for businesses, including financial losses, reputational harm, and legal liabilities (Jelacic). Credential fraud is an insider threat that happens when a worker or a third party with authorized access to a company's network uses stolen or forged credentials to access sensitive information or systems without authorization. This might happen due to social engineering schemes, phishing scams, or shoddy authentication processes. Credential fraud is a significant issue in the context of cloud migration because cloud services are frequently accessed remotely and businesses rely on authentication mechanisms to make sure that only authorized users have access to sensitive data. A successful credential fraud attempt may lead to malware infection, data exfiltration, or unauthorized access to sensitive information. Malicious insiders are employees or other authorized users who intentionally engage in activities that jeopardize the security of an organization's network, systems, or data. Malicious insiders may be driven by several motives, such as monetary gain, retaliation, or ideology. Malicious insiders can be a significant security risk in the context of cloud migration because they frequently have access to sensitive data kept in the cloud. The use of malicious insiders' access to steal, alter, or introduce malware into cloud services can lead to data breaches, financial losses, and reputational harm (Armerding).

DDoS Attacks

An example of a risk within cloud migration is DDoS attacks. A DDos attack or Distributed Denial of Service attack will take advantage of the specific amount of capacity limits on any network resource. DDoS attacks can cost up to $2 million per DDoS attack. The figure truly depends on the size of the organization. These steaks are getting higher as these firms and companies move towards the cloud and defending themselves from these DDoS attacks is very important (Jayaraman). Detecting these attacks through the cloud is essential for firms. Doing tests that can find and detect traffic patterns or the usage of resources. Spikes in traffic patterns can be flagged by the machine doing the testing as a warning of an attack. Companies use a Web Application Firewall (WAF) to automatically monitor traffic and give defense mechanisms to stop DDoS attacks from the cloud. Another way to detect attacks is to map out those signature attacks in the database, using it to recognize incoming attacks. Companies use a combination of these techniques to catch DDos attacks as they happen (Jayaraman).

Lack of Visibility and Control

According to Cypress Data Defense, lack of Visibility/Control is one of the major security challenges in cloud computing. The ease of implementing new servers and services can sometimes result in cloud deployments getting out of control. A lack of visibility in the cloud infrastructure can mean a loss of control over critical aspects of data security and IT management. This affects the organization's ability to enact incident response plans, verify the efficacy of their security controls, and properly assess information about their data, services, and users. It is crucial for organizations to have a cloud usage policy with approved mechanisms for getting approved servers stood up and deployment processes in place. A lack of visibility in the public cloud also poses business risks in terms of compliance, governance, and security. Maintaining strong compliance and security controls across the entire cloud infrastructure platform is important for preventing teams from deploying resources outside of the visibility of the security team.

Survey of Existing Solutions

Encryption

A possible solution to minimize the security risks when migrating to the cloud is encryption. When using cloud encryption, the data is sent to the cloud, however, it is made unreadable (encrypted) to those who are not supposed to access it. However, the data is then made readable (decrypting) for those with access to the data. (Zscaler, 2023 Copyright) This can be used to protect data when moving and not moving. Digital encryption was pioneered by David Chaum. He proposed the first blockchain back in 1981. The next year, Chaum would publish two papers, "one that proposed a protocol for making untraceable but unforgeable digital payments, the other showing a way to send untraceable email using a technique he called "digital pseudonyms." These papers were foundational to Chaum's later work on voting and conducting elections partly or completely online (Hamacher). Chaum's research would be critical in the creation of encryption for cloud services.

Cloud encryption works by encrypting the data using a key (or keys). A simplified example would be encrypting the word "difficult" to "inkknhzqy". In this example, the key is "5" since the encrypted version of each letter is made to be the fifth letter to the right of the original version. To decrypt we use the key in reverse. This version of encryption is called Symmetric Encryption. There is also Asymmetric Encryption, which uses key pairs. A public key is used to encrypt the data and a private key is used to decrypt it. The difference between the two is that the former is faster but less secure and the latter is slower yet more secure (Zscaler). That was the copyright date. The current estimated value of the cloud encryption market is US$ 3.1 billion. The cloud encryption market currently is around 4.5 percent of the total cloud security market ("Cloud Encryption Market").

Cloud encryption is effective. Its ability to protect data gives it strengths in a few areas. It ensures privacy, integrity (protection against data manipulation), verification, and regulation of data.

The weakness of cloud encryption is access to data and backup management. While cloud encryption protects data from attackers, this protection could slow down the data owner if they do not have access to the keys or passwords. It means that there needs to be a key management system to access the data. There also needs a backup system for the keys so the data/keys do not get lost in a worst-case scenario (Indeed Editorial Team).

Access Policies

Access policies can serve as a solution for security risks that companies may face when migrating to the cloud. Unauthorized access to sensitive data is one of the main security risks associated with moving to the cloud. When sensitive data is stored in the cloud, access policies can be used to guarantee that only authorized users can access it. This can be accomplished by implementing strong authentication measures such as single sign-on (SSO) and multi-factor authentication (MFA), as well as restricting access to sensitive data to employees who need it. Furthermore, to identify and stop unauthorized access, access policies can also be used to audit and monitor user access to sensitive data. Access controls that restrict access to sensitive information based on job function and monitoring tools that can spot unusual or suspicious activity can both help achieve this ("Create a cloud access policy").

Additionally, access policies may mandate that staff members create secure passwords and change them frequently. Last but not least, access policies can be used to track and log access to sensitive data and systems, enabling the early detection of potential threats and the detection of suspicious activity. In summary, access policies can serve as a solution for security risks that companies may face when migrating to the cloud.

Daily Framework Testing

The process of capitalizing on the cloud tools of a third-party service provider so you can simulate and assess the performance of your migrated applications is known as cloud migration testing. This testing will evaluate the requirements like availability, security, and scalability of the software. (Flash) These tests are very helpful in finding errors or perhaps intrusions into cloud migration. Testing within a cloud gives you the ability to check the internal features in the cloud to make sure that performances are optimal and are improving.

Testing servers can provide protection to the data that is used in the cloud. Preventing loss or any attack should be the main goal of these companies who are using cloud migration. Testing the Framework will provide a company safety with their cloud migrations from intruders and attacks and make sure that all data is transferred. Testing the migration process is a good way to find errors, errors that could lead to loss of data, always back up your data before it is transferred due to the migration process having the chance to error and lose that data but testing the frameworks of this process can help you see those errors and fix them and carefully manage all the data (Imperva). Security is crucial when it comes to cloud migration. Testing the framework can also point out certain attacks that are taking data or attempting to corrupt data, most of the time these attacks happen through a third-party migration process. Testing for the security of your data and network will prevent a lot of damage.

Making regular tests can help prevent the many risks that come with cloud migration and ensure that your data is encrypted and secure in the cloud. Stopping all those risks will make the process of migrating data simple and efficient.

Clear Communication Between Parties

As more businesses seek to streamline their operations, cloud computing has become an increasingly popular solution. However, implementing cloud computing services can be challenging, requiring effective communication between both the cloud service provider and the business. We can explore the importance of clear communication in offering cloud computing services to businesses.

To begin, effective communication enables the cloud service provider to understand the specific needs and requirements of the business. This allows them to tailor the service to the specific needs of the business, ensuring that they receive maximum value from the service.

Another benefit of clear communication is that it allows cloud service providers to address any concerns that the business may have about the security and privacy of their data. This can help to build trust between the two parties and facilitate a successful implementation.

During the planning and implementation process, clear communication is also essential. This allows both parties to work together to create a plan that meets the specific needs of the business. Additionally, ongoing training and support are crucial for the success of the cloud computing service, and clear communication enables the provider to provide this support effectively.

Finally, clear communication enables cloud service providers to ensure that the service remains flexible and scalable, meeting the changing needs of the business over time.

In conclusion, effective communication is crucial for the successful implementation and ongoing success of cloud computing services for businesses. It allows for tailoring the service to the specific needs of the business, addresses concerns, facilitates planning and implementation, and provides ongoing training and support. Overall, clear communication is the key to unlocking the benefits of cloud computing services for businesses.

Research Findings

The solutions proposed in this white paper, including encryption, access policies, regular security testing, and clear communication, are effective ways to mitigate security risks associated with cloud migration. However, there are still some gaps that need to be addressed. One issue that is not adequately covered by these solutions is the risk of fileless malware as previously mentioned. To reiterate, fileless malware is a type of malware that does not install anything on a computer but instead makes changes to existing files. This type of malware can be difficult to detect and can bypass traditional security measures. To address this risk, companies should consider using advanced endpoint detection and response (EDR) tools that can detect and respond to fileless malware. Another issue that needs to be addressed is the risk of insider threats. While the proposed solutions cover some aspects of insider threats, such as access policies and monitoring, they do not address the issue of credential fraud. Credential fraud occurs when an insider uses stolen or forged credentials to access sensitive information or systems without authorization. To address this risk, companies should consider implementing multi-factor authentication and other advanced authentication mechanisms. Overall, it is important for companies to understand that cloud migration presents a unique set of security risks that require proactive measures to mitigate. By using the solutions proposed in this white paper and addressing the gaps discussed above, companies can significantly reduce their risk of security breaches and protect their sensitive data and systems during cloud migration.

Works Cited

"12 Types of Malware + Examples That You Should Know." *Crowdstrike.com*, 4 Apr. 2023, https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/.

Arghire, ByIonut. "Several Law Firms Targeted in Malware Attacks." *SecurityWeek*, 1 Mar. 2023, https://www.securityweek.com/several-law-firms-targeted-in-malware-attacks/.

Armerding, Taylor. "Don't Let Insider Threats Rain on Your Cloud Deployment." *Application Security Blog*, 1 Oct. 2021, https://www.synopsys.com/blogs/software-security/insider-threats-cloud/.

"Cloud Encryption Market." *Future Market Insights*, https://www.futuremarketinsights.com/reports/cloud-encryption-market.

"Create a Cloud Access Policy." *Skyhigh Security*, 20 May 2022, https://success.myshn.net/Skyhigh_Data_Protection/Access_Control_Policies/Create_a_Cloud_Access_Policy.

6 Cloud Security Challenges and How to Address Them. https://www.cypressdatadefense.com/. Accessed 10 Apr. 2023.

Flash. "Cloud Migration Testing Guide: 8 Types and Benefits to Know." *Amzur*, 15 Nov. 2022, https://amzur.com/blog/types-of-cloud-migration-testing-methods#:~:text=What%20is%20cloud%20migration%20testing,performance%20of%20your%20migrated%20applications.

Hall, Gabriel E. "Law Firms Targeted in GootLoader and Fakeupdates Malware Campaigns." *Security and Spyware News*, 2-Spyware.com, 2 Mar. 2023, https://www.2-spyware.com/law-firms-targeted-in-gootloader-and-fakeupdates-malware-campaigns.

Hamacher, Adriana. “How David Chaum Went from Inventing Digital Cash to Pioneering Digital Privacy.” *Decrypt*, Decrypt, 6 Apr. 2022, https://decrypt.co/es/95109/david-chaum-from-inventing-digital-cash-to-pioneering-digital-privacy?amp=1.

“Introduction to Cloud Migration: Challenges, Tools & Strategies: Imperva.” *Learning Center*, 18 Mar. 2021, https://www.imperva.com/learn/application-security/cloud-migration/.

Jayaraman, Soundarya. “Battle in the Cloud: Preventing Ddos Attacks.” *Security Boulevard*, 1 Sept. 2022, https://securityboulevard.com/2022/09/battle-in-the-cloud-preventing-ddos-attacks/.

Jelacic, Bojan, et al. “Security Risk Assessment-Based Cloud Migration Methodology for Smart Grid OT Services.” *Acta Polytechnica Hungarica*, 1 Jan. 1970, https://scholar.archive.org/work/l63vdfiuofbgfo6k7bb6czzwma.

“Lumen Faces 2 Ransomware Attacks, Working with Experts to Evaluate and Minimize Impact.” *Yahoo! Finance*, Yahoo!, 27 Mar. 2023, https://finance.yahoo.com/news/lumen-faces-2-ransomware-attacks-173955639.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAH3bGPq9o-pREdTi0zWO3Efiyjtp1sbbsfxWj3LvROKn8JuUmg7L29J11uPP7AGuIY8HpksqroWVNG5q4TH_UxhpAn5izKDhrHDE-di2j_LSMgS8faZ3uki7OmBYxFpCu2FxySOQzhDSNm7L7IyamW1cflRJKa2Swu0gc067h9tx.

Montalbano, Elizabeth. “Google: Commercial Spyware Used by Governments Laden with Zero-Day Exploits.” *Dark Reading*, 29 Mar. 2023, https://www.darkreading.com/attacks-breaches/google-spyware-governments-zero-day-exploits.

“What Is Cloud Encryption? Encrypted Cloud Storage Benefits.” *Zscaler*, 2023, https://www.zscaler.com/resources/security-terms-glossary/what-is-cloud-encryption#:~:text=Cloud%20encryption%20is%20a%20data,or%20at%20rest%20against%20cyberattacks.

“What Is Encryption? Types, Benefits and How It Works - Indeed.” *Indeed*, 8 Aug. 2022, https://www.indeed.com/career-advice/career-development/what-is-encryption.