Introduced Vulnerabilities through Rehosting

legacv
Computer and Information Technology
Purdue Polytechnic Institute
West Lafayette, USA

***Abstract*—When organizations choose to move their on-premises infrastructure to the cloud, they may choose a rehosting migration. Rehosting is not an ideal solution not only for its low ROI, but also for the vulnerabilities it introduces into a cloud environment. Network- and identity-based threats become more common through this method, and it is recommended that when organizations migrate, they choose to adapt their architecture to adopt security services made for cloud environments.**

***Index Terms*—cloud computing, cloud security, penetration testing, rehosting**

I. Introduction

Cloud-based infrastructure has become an increasingly attractive option for small- to medium-sized businesses in the past decade. A lower barrier to entry and lower maintenance costs due to a reduced need for network engineers, hardware replacement, and datacenter cooling can entice newer businesses to buy their infrastructure from Infrastructure-as-a-Service (IaaS) providers such as Amazon Web Services (AWS), Azure, Google Cloud, DigitalOcean, and more. Older, more established businesses that may already work with on-premises infrastructure, however, must perform a migration in whole or in part in order to reap the benefits cloud providers have to offer.

Providers know this, and have capitalized off it; the size of the cloud migration market in 2025 is USD 0.3 trillion, with some estimates expecting it to grow to USD 1.03 trillion by 2030 at a compound annual growth rate (CAGR) of 28.24% [1]. Although migration may be a worthwhile investment in the long term, the short term presents unique challenges; the larger the business or migration, the more challenging it is to plan for and execute. The sector of industry the company operates in also must be taken into account; if customers' personally identifiable information (PII), personal health information (PHI), or payment card information (PCI) data must be migrated, that migration must be secure in order to minimize the chances of data loss and theft. In addition, moving to new infrastructure always has the possibility to introduce vulnerabilities into an ecosystem, whether through misconfiguration, user error, or architecture mismatch.

Therein lies the central security concern. What kinds of security vulnerabilities and architecture flaws is cloud migration most likely to create in a company's infrastructure, and how can they be effectively mitigated? This question guided research for this paper while also looking to incorporate themes of identity and access management (IAM), attention to detail, and attacker perspectives on these migrations, with the final objective being to discover what vulnerabilities the rehosting migration strategy introduces into a company's environment that wouldn't have existed if the company had persisted with on-premises infrastructure.

It is important to note that the topic is not what risks arise from cloud hosting in general, but specifically how a rehosting migration can degrade the security posture of an organization due to unfamiliarity with cloud security features during said migration.

A. Source Selection

Academic research papers on topics such as penetration testing in the cloud and best practices for cloud migration were sought out as references from Google Scholar, using keywords such as "cloud," "migration," "penetration testing," "rehosting," "case study," and combinations of the aforementioned. In addition, white papers from organizations such as the National Institute of Standards in Technology (NIST), AWS, Google Cloud, and Microsoft were used for mitigation recommendations. Finally, research from companies such as O'Reilly, Mordor Intelligence, and Accenture was used to provide statistics on current trends in the cloud industry.

II. Background

A. Cloud Migration Strategies

There exist six common terms for the modification of on-premises infrastructure with respect to cloud environments, four of which refer to the movement of networks and data into the cloud [2]:

- Rehosting: Also known as lift-and-shift. The process of moving on-premises infrastructure to a 1:1 copy of itself hosted by an IaaS provider.
- Replatforming: Optimizing migrated applications and infrastructure such that they implement some native features of the cloud, including those related to security and performance.
- Refactoring: The complete redesign of infrastructure from scratch in order to integrate cloud-native features and optimize applications for a cloud environment.
- Repurchasing: Replacement of an application with a cloud-native likeness that accomplishes a similar purpose, often from a Software-as-a-Service (SaaS) provider.
- Retiring: Choosing to retire unnecessary applications.
- Retaining: Not moving certain pieces of infrastructure to the cloud due to budgetary or technical constraints.

The paper is concerned with the first item, rehosting, otherwise known as the lift-and-shift approach. It is often the simplest option for companies for which it would be technically infeasible or too time-consuming to recreate architecture. As will be discussed, however, it is prone to creating weak points in infrastructure due to its oversight of cloud-native security features.

B. Historical Trends in Cloud Migration

As of 2020, 88% of businesses surveyed by O'Reilly used the cloud in one form or another, with most expecting to increase their usage. 25% of those surveyed claimed they were planning to move all of their content to the cloud – or, in other words, migrate [5]. More recent 2025 figures by Flexera that surveyed cloud-using businesses revealed that data warehouses were the top use for cloud providers, followed by Database-as-a-Service (DBaaS) and Container-as-a-Service (CaaS). In addition, the second most widespread cloud challenge businesses reported was security, following managing cloud spending [6].

Exact statistics on what amount of migrations planned were rehosts vs. replatforms vs. refactors are hard to obtain, as businesses do not tend to reduce their entire migration strategy to one word – though, if it were necessary, the majority of migrations would most likely be classified under replatforms. Many case studies, such as those done by Accenture, highlight how a company's base architecture stayed in the same form, with some adoption of cloud-native security and performance features in order to obtain a positive return-on-investment (ROI). Accenture themselves adopted a hybrid cloud approach through rehosting [7], and reported on the California Statewide Automated Welfare System's (CalSAWS) movement into the cloud in order to increase program efficiency [8]. Both of these case studies emphasized the fact that while the primary and ancillary databases, etc. remained the same, incremental architecture changes to adopt cloud-native services were capitalized upon in order to improve efficiency.

This is to say, modern businesses do not often migrate using a fixed lift-and-shift approach, as this does not often provide positive ROI [6]. Despite this, companies focused on the short-term, or those that are on small budgets and short timelines, may choose it due to its smaller workload and less customization needed from their engineers. As mentioned, this failure to adapt may lead to security vulnerabilities that opportunistic attackers take advantage of and use to breach a company's systems.

It is unknown how many security breaches result from cloud migrations each year, as the figure is difficult to quantify. Finding such a figure would require industry-wide analysis on which companies have recently completed migrations, which of those have suffered a successful attack on their data systems, and a subsequent root cause analysis (RCA) on whether or not their new, cloud-based systems were truly the point of failure. Nevertheless, theoretical analyses of the increased risk migration brings on are vital for companies to calculate their risk appetites accordingly.

III. Weaknesses in Rehosting Migrations

A. Potential Security Flaws

1) Improperly segmented networks: When organizations rehost, they often replicate their existing on-premises network structure directly into the cloud environment, which is typically designed around a traditional perimeter-based security model. When rehosted, features such as Virtual Private Clouds (VPCs), subnet isolation, and the use of network security groups go unutilized. Failure to change an architecture to adopt these tools can result in weak internal boundaries, which allows attackers to pivot between clusters, nodes, machines, and services much more effectively.

2) Identity and access management flaws: On-premises infrastructures often rely on local accounts or directory services for access management, as well as service accounts. When migrating, these access controls are typically left unchanged, which bypasses the use of cloud-native IAM tooling and frameworks. The tenets of zero-trust, least-privilege, just-in-time credentialing, etc. are lacking, and as such create blind spots wherein system administrators may not know exactly how much access a given user or service account has to the new cloud infrastructure. Further down the line, these gaps limit an organization's ability to enforce best practices in modern access control, like those mentioned above.

3) Insecure secret storage: Legacy applications are often configured to use hardcoded credentials stored in configuration files or environment variables due to the on-premises access control policies of the organization. When rehosted, these insecure methods can be retained, despite the availability of cloud-native services designed for secure secret management. Unnecessary risk is introduced through this vector; plaintext secrets can be leaked via logs, version control, or compromised hosts. Attackers that obtain these credentials, API keys, etc. could gain persistent access to sensitive systems or data, especially if secrets are not regularly rotated.

4) Default container orchestration: Virtualization and containerization are core tenets of IaaS cloud offerings and architecture. When creating VM mappings of physical infrastructure or containerizing services, softwares like Docker and Kubernetes often don't come with security features enabled in order to maximize ease-of-use for their users. Permissive pod security policies, default passwords, and exposed administrative interfaces can, if not dealt with, become effective vectors for attackers to gain access to administrative actions on a cluster or machine. Inadequate isolation between pods or namespaces, as defined in 1), can further exacerbate the damage caused by insecure container or cluster configuration.

5) Improper asset management: Tagging and metadata strategies are important to solidify and abide by during the creation of a cloud architecture. An unwillingness to properly label and describe storage, containers, virtual machines, resource groups, etc. can lead to pieces of architecture being neglected and forgotten, which allows them to: become stale, not receive the latest patches, not be logged and monitored correctly, and not be factored into cost calculations. The

business impact of forgotten infrastructure is high, and of course, comes with added risk; machines and software that don't receive patches and security updates become attack vectors.

6) Insecure cloud storage: IaaS providers serve different types of data storage, with some of the most well-known being AWS S3 buckets, Azure Blob Storage, and Google Cloud Storage. Moving data directly to these storage solutions without proper consideration of the types of user and service account access policies that should be implemented allow for data leaks – therefore, this could be considered an offshoot of IAM flaws. Many services exist to look for misconfigured or public S3 buckets that host secrets, and bots constantly scrape for newly-published, insecure cloud data; therefore, before a new cloud architecture even goes live, a thorough audit of data access policies is necessary.

B. Available Security Opportunities

There were three major IaaS cloud providers selected for review: Microsoft Azure, Google Cloud, and Amazon Web Services (AWS). All three providers provide extensive documentation for the secure setup of cloud systems, and some provide prescriptive guidance for the adoption of the cloud.

AWS, for example, has prescriptive guidance in the form of Security Reference Architecture that details the tools, techniques, and procedures available to network administrators to implement zero-trust architecture. These include [9]:

- VPC Lattice
- AWS PrivateLink
- AWS Network Firewall
- AWS Identity and Access Management (IAM)
- AWS Verified Access
- VPC Flow Logs and AWS CloudTrail
- AWS STS and Secrets Manager
- AWS Config and Security Hub

The web version of the prescriptive guidance also has an option to sort reference articles by migration type, including rehosting. The articles include information on how to transfer on-premises MySQL, MariaDB, and other databases to their AWS equivalents, and the same information for other infrastructure such as virtual machines.

In addition, there exists the AWS Well-Architected Framework (AWS WAF), which optimizes "operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability" [10]. The Framework is supported by the built-in AWS Well-Architected Tool which asks a series of questions to determine whether a workload is in line with the AWS WAF.

Azure and Google Cloud both have similar white papers and documentation that describe best practices for using their cloud services.

Azure provides tools such as [12]:

- Microsoft Entra
- Application Security Groups
- Microsoft Sentinel
- Network Security Groups for VNets
- Azure Firewall

While Google Cloud provides items such as [13]:

- Google Cloud Armor
- Shared VPC
- VPC Service Controls
- Cloud IDS
- Workload Identity Federation

Combinations of these tools, wielded properly by system administrators and cloud engineers, could allow for the creation of an effective zero-trust architecture. Many of them depend upon being built into an architecture as it's being created; it's more difficult to create a firewall ruleset for the dozens of services being hosted after they are all configured than to create and test rules individually while the services are being implemented.

C. In the Wild

A handful of organizations have dedicated themselves to enumerating and classifying the most common vulnerabilities that exist in cloud environments. Further reading on the topic can be done through the Open Web Application Security Project, which has classified the top 10 cloud-native application risks, quoted below from [4]:

> "1) Insecure cloud, container or orchestration configuration
> 2) Injection flaws (app layer, cloud events, cloud services)
> 3) Improper authentication & authorization
> 4) CI/CD pipeline & software supply chain flaws
> 5) Insecure secrets storage
> 6) Over-permissive or insecure network policies
> 7) Using components with known vulnerabilities
> 8) Improper assets [sic] management
> 9) Inadequate 'compute' resource quota limits
> 10) Ineffective logging & monitoring (e.g. runtime activity)"

These have significant overlap with the items mentioned in section III.A Potential Security Flaws. IAM misconfigurations, insecure container configuration, improper asset management, and ineffective monitoring are all side effects of an improperly conducted cloud migration in which the native features of the cloud are barely or only mildly considered. These are also symptoms of analysts, engineers, or architects who are poorly-adjusted to the cloud; logging and monitoring of virtual machines, nodes, pods, clusters, microservices, and other virtualized and containerized technologies can often be much different than the monitoring of physical hardware and servers, and can have a steep learning curve.

In addition, for those who regularly monitor and administer cloud environments, the cloud security company Wiz maintains a database of CVEs that affect cloud security providers and applications called the Cloud Vuln DB. Many of these vulnerabilities are found actively exploited in the wild (EITW), and vendors often provide patches or fixes that are posted with

the CVE as soon as they are available [14]. Keeping pace with the vulnerabilities relevant to a business's architecture is vitally important to ensure business longevity and reduce risk created by passivity.

IV. Recommendations and Mitigation

Each cloud provider has their own recommendations for organizations developing a cloud infrastructure to take into account. The documentation from providers such as AWS, Google, and Microsoft mentioned in III.B Available Security Opportunities is of utmost importance to reference throughout the process of rehosting.

When rehosting, other best practices to follow include [2]:

- Outlining a defined scope and setting realistic expectations for migration
- Engaging key stakeholders, including users
- Internal transparency between teams during migration
- Adopting a phased migration approach
- Ensuring regulatory compliance during and post-migration
- Auditing data pre- and post-migration
- Continuous, frequent testing of migrated services and applications
- Investing resources into upskilling and reskilling

In addition, it is important to train personnel on effective cloud management, maintenance, and monitoring. The vulnerabilities introduced by migration are rarely products of insecure virtualization or containerization software, but rather misconfiguration or lack of awareness on the part of those performing the migration. An unwillingness to implement zero-trust architecture, trading security for ease-of-use, an underfunded migration or team, or an exceedingly quick timeline all present opportunities to cut corners, leading to improper configurations that attackers could potentially exploit. Finding the architecture reference and security best practices for the IaaS provider(s) being used and implementing them helps improve a cloud-based organization's security posture and resiliency against threats.

Finally, if budget and time constraints allow for it, it is recommended to consider an alternative cloud migration method such as replatforming or even refactoring. Leaving systems unchanged during an architecture shift is not, in the author's view, best practice.

V. Conclusions and Future Work

It is the position of the author that rehosting should not be used as an enterprise cloud migration tactic, not only due to the missed opportunities for architecture efficiency, but also for the attack vectors that rehosting introduces into the environment. They allow for attackers to access and pivot on a cloud network much more easily through a combination of untended servers, improperly segmented networks, high-privilege user and service accounts, exposed secrets and data, and more. Future possible work includes expansion on the themes previously mentioned in the paper. These may include hands-on exploitation of the attack vectors listed; simulations of enterprise infrastructure and data migration in order to study their minutiae; more thorough case studies conducted through communication with companies that have rehosted their architecture; communication with companies that have performed penetration tests on recently rehosted architecture; and more. Further statistics and research data could prove useful to dissuade enterprises from rehosting. Of course, effective alternatives would have to be provided; not every company has the means to rebuild their architecture from scratch, especially if the migration is on a short timeline. In addition, an exploration of the attack vectors introduced through other types of cloud migration, such as refactoring, could prove worthwhile.

Acknowledgment

The author thanks the professor for his guidance and Tyler for the inspiration for this paper, as well as Colin for his support.

References

[1] Mordor Intelligence Research & Advisory. "Cloud Migration Market Size - Industry Report on Share, Growth Trends & Forecasts Analysis (2025 - 2030)," Mordor Intelligence. https://www.mordorintelligence.com/industry-reports/cloud-migration-services-market

[2] S. Chinamanagonda, "Cloud Migration Strategies and Best Practices," SSRN Electronic Journal, 2024, doi: https://doi.org/10.2139/ssrn.4986770.

[3] A. Khajeh-Hosseini, D. Greenwood and I. Sommerville, "Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS," 2010 IEEE 3rd International Conference on Cloud Computing, Miami, FL, USA, 2010, pp. 450-457, doi: 10.1109/CLOUD.2010.37.

[4] "OWASP Cloud-Native Application Security Top 10," OWASP. https://owasp.org/www-project-cloud-native-application-security-top-10/

[5] R. M. Swoyer Steve, "Cloud Adoption in 2020," O'Reilly Media, May 19, 2020. https://www.oreilly.com/radar/cloud-adoption-in-2020/

[6] "Flexera 2025 State of the Cloud Report," Flexera, 2025. [Online]. Available: https://info.flexera.com/CM-REPORT-State-of-the-Cloud

[7] S. Gooch and D. Galzarano, "Cloud Security Case Study: Zero Trust Strategy — Accenture," www.accenture.com. https://www.accenture.com/us-en/case-studies/about/cloud-security

[8] Accenture, "CalSAWS takes first step in cloud journey," Accenture.com, Jun. 02, 2023. https://www.accenture.com/ca-en/case-studies/public-service/calsaws-cloud-journey.

[9] Global Services Security Team, Amazon Web Services, AWS Security Reference Architecture, AWS Prescriptive Guidance, Amazon Web Services, Inc., Sept. 2024. [Online]. Available: https://docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/

[10] Amazon Web Services, AWS Well-Architected Framework. [Online]. Available: https://aws.amazon.com/architecture/well-architected/

[11] Amazon Web Services, Overview of the AWS Cloud Adoption Framework, Whitepaper, Apr. 2023. [Online]. Available: https://docs.aws.amazon.com/pdfs/whitepapers/latest/overview-aws-cloud-adoption-framework/overview-aws-cloud-adoption-framework.pdf

[12] Microsoft, Plan for security in the Cloud Adoption Framework. [Online]. Available: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/plan

[13] Google Cloud, Cloud Architecture Center. [Online]. Available: https://cloud.google.com/architecture/

[14] "The CVE Database: Curated Vulnerability Intelligence by Wiz — Wiz," wiz.io, 2025. https://www.wiz.io/vulnerability-database