Capgemini engineering

BEST PRACTICES FOR SECURE CLOUD MIGRATION

How to Close the Security Gap of Your Transition to the Cloud

Table of Contents

Executive Summary

Moving to the cloud is not just a technology change, it is a cultural change that impacts the entire business. Due to the cloud's superior flexibility, scalability, security and business continuity services, workloads are migrated from on-premises to the cloud. But the errors and misconfigurations that can occur during and after cloud migration run the risk of creating a higher level of security threats than the on-premises solution.

Security is vitally important for businesses planning to transition seamlessly to the cloud. However, according to the Oracle and KPMG Cloud Threat Report 2020, cloud migration outpaces security readiness.[1] "The sheer rate at which the use of cloud services is expanding is creating an appreciable cloud security readiness gap," according to the report. A staggering 92% of the study's respondents admitted their organization has a gap between current and planned cloud usage and the maturity of their cloud security. What's more, an alarming 44% of respondents said the gap was wide.

This whitepaper discusses how to close the security gap by managing the strategy, compliance and implementation risks of migrating to the cloud. We offer recommendations for raising organizational awareness of the importance of having a comprehensive, robust cloud security plan in place before making a move.

[1.] "Oracle and KPMG Cloud Threat Report 2020," Oracle and KPMG, https://www.oracle.com/security/cloud-threat-report-2020.html

Why Cloud Security?

In 2020, the worldwide Covid-19 pandemic accelerated the pace of organizations migrating to the cloud. During the first quarter of 2020 alone, cloud spending rose 37% to $29 billion.[2]

Unfortunately, these migrations do not always go as planned. There is a higher risk of data loss during migration and misconfiguration and improper access control, both of which can result in a data breach. To minimize the security risks and threats, it is vital to take security precautions through all the migration phases.[3]

Hackers follow the money. So if the cloud is where the action is, that is where they will be. Indeed, many hackers buy on-demand cloud capabilities to underpin their offensive operations, meaning they are using the cloud to exploit the cloud.[4]

Here are 13 ways hackers can access your cloud data.[5]

Data Breach: A data breach exposes confidential, sensitive or protected information to an unauthorized person. The consequences for businesses that experience data breaches are severe and increasing. In general, data breaches occur due to weaknesses in user behavior and the technology used.

Data Loss: Data loss often happens due to natural or manmade disasters, the physical destruction of the servers, human error or the result of a targeted attack. Regardless of the cause, you lose all of the data you've been collecting for years.

Lack of Cloud Security Architecture and Strategy: No matter how big or small the enterprise, proper security architecture and strategy are required elements for securely moving, deploying and operating in the cloud. A successful cyberattack can severely impact a business, including financial loss, reputational damage, legal repercussions and fines.

Weak Control Plane: Migration from the data center to the cloud has some challenges for creating a sufficient data storage and protection program. The solution for these problems would be a control plane as it enables the integrity and security that would complement the data plane that provides stability and runtime of the data. A weak control plane may result in data loss, and users may be unable to protect their cloud-based business data and applications.

Metastructure and Applistructure Failures: Metastructure and applistructure are critical components of a cloud service. Failures involving these features at the Cloud Service Provider (CSP) level can severely impact all service consumers. At the same time, misconfigurations by the tenant could disrupt the user financially and operationally.

Limited Cloud Usage Visibility: Limited cloud usage visibility happens when the organization cannot analyze and visualize if the cloud service use within the organization is safe. This can put organizational data, services and finances at risk.

[2.] "Can you meet customer demand for cloud-based computing?" https://www.pwc.com/us/en/industries/tmt/library/covid19-cloud-infrastructure.html#:~:text=A%20confluence%20of%20existing%20factors,the%20first%20quarter%20of%202020

[3.] Randall, Erik "5 Steps to Ensure Your Cloud Migration is Secure," Dec. 12, 2019, Exabeam https://www.exabeam.com/how-to/5-steps-to-secure-your-cloud-migration/

[4.] «Top Threats to Cloud Computing: The Egregious 11," Aug. 6, 2019, Cloud Security Alliance https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/

[5.] Chaudhary, Ashwin «Cloud Security Challenges in 2020,» Feb. 18, 2020, Accedere Inc. and the Cloud Security Alliance https://cloudsecurityalliance.org/blog/2020/02/18/cloud-security-challenges-in-2020/

Insecure Interfaces and APIs: APIs and UIs are generally the most exposed parts of a system, perhaps the only asset with a public IP address available outside the trusted organizational boundary. Therefore, security by design and adequate controls protecting them from attacks is required. Relying on a weak set of interfaces and APIs exposes organizations to various security issues related to confidentiality, integrity, availability and accountability. Additionally, regulatory and financial impacts could be very significant.

Insider Threat: An insider threat is "the potential for an individual who has or had authorized access to an organization's assets to use their access either maliciously or unintentionally, to act in a way that could negatively affect the organization," according to the Software Engineering Institute.[6] Insider threats can result in the loss of proprietary information and intellectual property. System downtime associated with attacks can negatively impact company productivity.

Cryptojacking: In this type of attack, hackers use your computing resources to process cryptocurrency transactions by installing a crypto mining script on your servers without your consent. This leads to an increased CPU load and, as a result, can significantly slow down your system.

Distributed Denial of Service (DDoS): A DDoS attack is a malicious attempt to disrupt the normal traffic on a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic. Such an attack can prevent regular traffic from arriving at the service and may result in downtime.

Account Hijacking: This is a threat in which malicious attackers gain access to and abuse highly privileged or sensitive accounts. In cloud environments, the accounts with the highest risks are cloud service accounts and subscriptions. Account hijacking consequences include data leaks that lead to reputational damage, brand value degradation, legal liability exposure and sensitive personal and business information disclosures.

Improper Access Management: Malicious actors masquerading as legitimate users, operators or developers can read, exfiltrate, modify and delete data; issue control plane and management functions; snoop on data in transit; and release malicious software that appears to originate from a legitimate source. As a result, improper access management can enable unauthorized access to data and lead to potentially catastrophic damage to organizations and end-users.

Cloud Misconfigurations: Misconfiguration happens when computing assets are set up incorrectly, leaving them vulnerable to malicious activities. A leading cause of data breaches is misconfiguration of cloud resources and can allow deletion or modification of resources and service interruption.

[6.] "Insider Threat," Software Engineering Institute, Carnegie Mellon University https://www.sei.cmu.edu/our-work/insider-threat/#:~:text=Insider%20Threat%20%5Bis%5D%20the%20potential,could%20negatively%20affect%20the%20organization.

Five Steps to Keep Your Cloud Operations Secure

This section details the five-step process you need to follow to successfully transition from an on-premises data center to a safe, secure cloud environment.

Step 1: Plan Secure Cloud Migration and Baseline Security

Before migrating to the cloud, implement a central security policy that spans all workloads. Once the policy is in place, perform a gap analysis for how the cloud will change your security paradigm. Also, you will need to verify how migrating to the cloud will impact risk management.

Create architectures of your current workloads that you plan to migrate, keeping in mind how security is incorporated in your existing workloads. This step will help you define and include cloud security when migrating to the cloud.

Use reference architectures for your cloud platforms. These architectures will help you plan the migration and provide guidelines for incorporating cloud security at the architectural level.

Step 2: Conduct a Data Compliance Assessment for the Cloud

Many organizations mistakenly assume that once the data has migrated to the cloud, all security and compliance responsibility shifts to the CSP. This is not the case.

You need to know the regulatory requirements that apply to your data before migrating it to the cloud. (See Figure 1.) Most CSPs are compliant with industry-standard certifications. However, you still need to meet compliance requirements for your data.

Public cloud providers, such as Amazon Web Services (AWS), Google Cloud Platform (GCP) and Microsoft Azure, have cloud services for the customer to verify their cloud workloads are compliant. These services also help with the remediation of non-compliant resources and services and help users achieve the desired regulatory compliance.

One useful resource to help choose a CSP is the 14 Cloud Security Principles, which is part of the UK's Cloud Security Guidance. (See Figure 2.) [7]

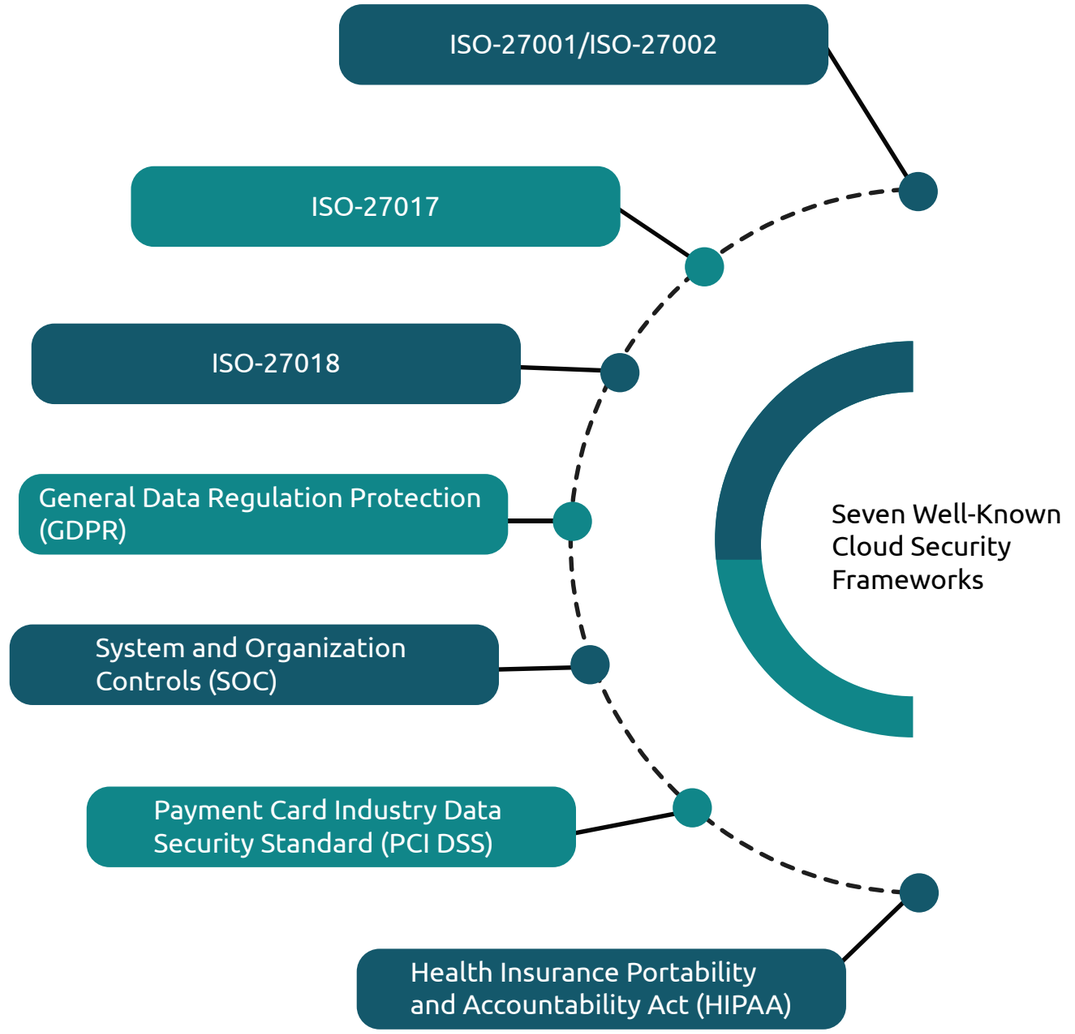

Figure 1: Know the Regulatory Security Requirements for Your Data Before Migrating to the Cloud
Compiled by Capgemini Engineering

[7.] "Cloud Security Guidance ," UK National Cyber Security Centre
https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles

1. **Data In Transit Protection:** User data transiting networks should be adequately protected against tampering and eavesdropping

2. **Asset Protection and Resilience:** User data, and the assets processing it, should be protected against physical tampering, loss, damage or seizure

3. **Separation Between Users:** A malicious or compromised user should not be able to affect the service or data of another

4. **Governance Framework:** The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined

5. **Operational Security:** The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes

6. **Supply Chain Security:** The service provider should ensure that its supply chain supports all of the security principles satisfactorily which the service implements

7. **Personnel Security:** When service providers have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel

8. **Secure Development:** Services should be designed and developed to identify and mitigate threats to their security. Those which are not may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity

9. **Secure User Management:** Your provider should enable you to securely manage their service and make the right tools available. Management interfaces and procedures are a critical part of the security barrier, preventing unauthorized access and alteration of your resources, applications and data

10. **Identity and Authentication:** All access to service interfaces should be constrained to authenticated and authorized individuals

11. **External Interface Protection:** All less trusted interfaces should be identified and appropriately defended

12. **Secure Service Administration:** Systems used for administration of a cloud service should have highly privileged access. The compromise of these systems would have a significant impact, including the means to bypass security controls and manipulate or even steal large volumes of data

13. **Audit Information For Users:** You should be given the audit records required to monitor access to your service and the data within it. Your ability to detect and respond to malicious activities within reasonable timescales will depend on the type of audit information available

14. **Secure Use of the Service:** The security of cloud services and the data within them can be weakened if you use the service inefficiently. Consequently, you will have responsibilities while using the service for your data to be adequately protected

Figure 2: Implementing the UK Cloud Security Principles
Source: UK National Cyber Security Centre

Step 3: Adopt a Shared Responsibility Model on the Cloud

CSPs operate under a shared responsibility model. To ensure that your migration is secure, you need to know who is responsible for which aspect of the plan. There are three main types of cloud services: Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS). Simply put, using IaaS, customers are provided with computing resources capable of accessing and monitoring computers, storage, networking, etc. PaaS refers to cloud services that provide a framework that companies and developers can use to quickly and easily build and customize applications. And SaaS uses the internet to deliver applications, which are managed by a third-party vendor, to its users.[8] Figure 3 highlights how the responsibilities split between the on-premises model and the three cloud models.

If you need more control over the infrastructure, then IaaS should be your choice. PaaS can streamline workflows when multiple developers are working on the same development project. SaaS provides numerous advantages to companies and employees by significantly reducing the cost and time spent on tedious tasks such as installing, upgrading and managing software.[9]

Cloud-native security services are offered for all the functions you are responsible for. In most cases, the services offer more robust, fine-grained security controls than you can provide on your own.

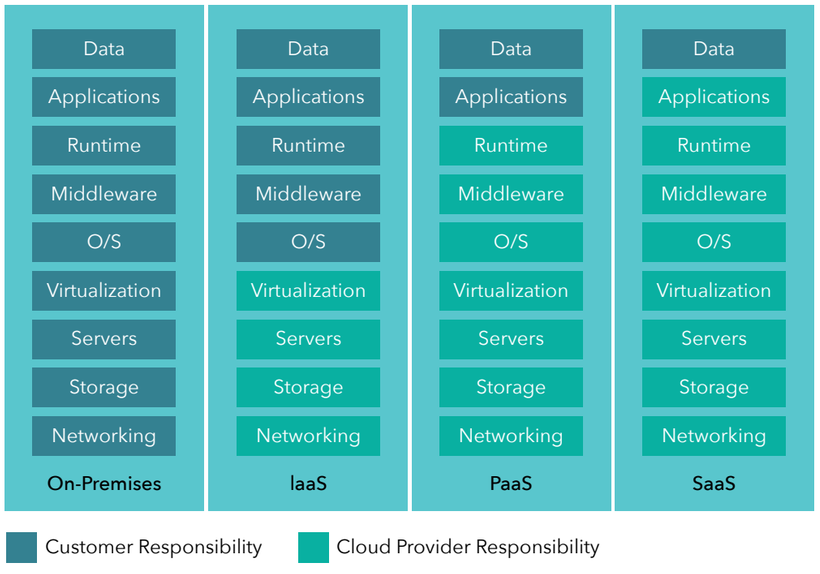

Figure 3: Shared Responsibility Model Options in the Cloud
Source: Capgemini Engineering

[8.] Randall, Erik "5 Steps to Ensure Your Cloud Migration is Secure," Dec. 12, 2019, Exabeam https://www.exabeam.com/how-to/5-steps-to-secure-your-cloud-migration/

[9.] Watts, Stephen, Raza, Muhammad, «SaaS vs PaaS vs IaaS: What's the Difference & How to Choose,» Jun. 15, 2019 BMC Software https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/

Step 4: Map the Migration Strategy

There are three phases in the migration strategy: Assessment, Mobilization and Phased Migration.

Phase 1: Assessment

First, identify the outcomes you need for your business, for example, financial outcomes, performance-based outcomes and scalability-based outcomes. The metrics you choose will be the basis for developing the business case for migration. For example, the company's data center consumes a large percentage of the annual IT budget. If IT chooses to conduct a cloud migration and transitions the assets in that data center to an IaaS solution, the company will realize a three-year cost reduction.

Next, verify your current readiness for working on the cloud with a specific CSP. Services and tools provided by CSPs can access your current environment, project the cost of the workloads and determine when they will be migrated to the cloud. Verify which areas can be migrated as they are, or if they need improvements and modifications beforehand.

Phase 2: Mobilization

n this phase, you will define a migration plan based on your business requirements. If required, you can refine the business case. You need to identify the gaps, improvements and modifications needed in your environment that were discovered during the assessment phase. Also, start planning how to build your baseline environment and train your organization to have the relevant cloud skills.

Now you are ready to create a migration plan. Keep in mind the applications, servers, legacy applications, etc., currently being used and identify any dependencies and interdependencies. Next, plan your migration using the six most common strategies of cloud migration.[10] [11]

1. **Rehost:** Also known as Lift and Shift, this involves lifting your stack and shifting it from on-premises hosting to the cloud.

2. **Replatform:** This is a variation of Lift and Shift that involves making a few further adjustments to optimize your landscape for the cloud.

3. **Refactor:** Refactoring, or rearchitecting, means rebuilding your applications from scratch.

4. **Repurchase:** This means moving your applications to a new, cloud-native product, most commonly a SaaS platform, for example, moving a CRM to the cloud.

5. **Retire:** Once you have assessed your application portfolio for cloud readiness, you may find some applications that are no longer useful. In this case, simply turn them off. The resulting savings might boost your business case for applications that are ready for migration.

6. **Retain:** During a cloud migration process, you may decide to retain portions of your IT portfolio. For example, you have some applications you aren't ready to migrate to the cloud and feel more comfortable keeping them on-premises. In this use case, it makes sense to retain aspects of your IT services in its current environment and implement a hybrid or partial migration strategy.

[10.] Orban, Stephen, "6 Strategies for Migrating Applications to the Cloud," Nov. 1, 2016, AWS Cloud Enterprise Strategy Blog https://aws.amazon.com/blogs/enterprise-strategy/6-strategies-for-migrating-applications-to-the-cloud/

[11.] webpage, "What Is a Cloud Migration Strategy?" Cisco https://www.cisco.com/c/en_in/solutions/cloud/what-is-a-cloud-migration-strategy.html#~strategies

Phase 3: Phased Migration

Creating a proof of concept (POC) is the first step in executing the cloud migration in almost all cases. POC will not anticipate all possible issues, but it will give you greater clarity and understanding of the problems you might come across.

Phased migration is a practical approach that starts by moving small and low-risk workloads to the cloud first. This ensures that workloads migrate in a controlled manner with minimal risk. Next, test your implementation to detect any security bugs and misconfigurations so you can remediate them before migrating your high-priority data. Another advantage of the phased migration approach is that implementation and configuration occur at a slower pace, which reduces the security risk.

During the migration process, there is a chance that customer data may get deleted or stored in the wrong place due to poor data migration practices. The other case would be damage due to changes in data security levels. This could result in access to data by unauthorized persons. You must ensure proper security measures and continuous monitoring of the workloads are in place.

Step 5: Cloud Security Implementation and Configuration

Cloud security is very different than traditional security in the on-premises environment. That is because the tools and processes used in the old environment are not fully applicable to the new cloud environment.

On-premises security typically involves a perimeter defense approach around the entire infrastructure. There are several challenges with this approach when implementing it in the cloud. For example, it does not adapt to the continually evolving sophisticated threats and attack vectors.

Also, by default, everything in the cloud environment is connected with different services in the infrastructure and across the internet. Therefore, a traditional on-premises approach to security is not recommended. Cloud security is a service-oriented architecture. It is integral to all stages, from design and development to operations. The zero-trust security model and the DevSecOps concept of baking security into the engineering process early on should be used in cloud migration and infrastructure.

Before the migration begins, the necessary infrastructure should be created in the cloud. Only after this infrastructure has been secured should the migration begin.

Cloud security requires the implementation and configuration of many security solutions, including a firewall, Web Application Firewall (WAF), Identity and Access Management (IAM), Encryption, Cloud Access Security Broker (CASB) and others.

When choosing the security tools and services, keep in mind your post-migration needs. It might seem easier to rely on some tools just for migration purposes and upgrade and modify them post-migration. However, this approach might leave significant gaps in your security postures, such as limited cloud usage, visibility, improper access management and cloud misconfigurations. Also, cloud migration can take longer than expected due to unexpected delays or unplanned issues, which may lead to security gaps lasting longer than intended.

Ten Cloud Security Recommendations

Below is a list of the most important actions you should take to ensure the migration from on-premises to the cloud is smooth and secure.

1. Identity and Access Management: Maintain proper access control on the cloud, always follow the principle of least privilege and only allow the necessary users or services to access your administrative services.

2. Data Encryption: Ensure data-at-rest and data-in-transit are encrypted.

3. Cloud Vulnerability Assessment and Penetration Testing (VAPT): Perform routine vulnerability assessments and penetration testing on your cloud environment.

4. Isolation of Workloads: Isolate different workloads from each other. Unless required, different services and workloads should not be allowed to communicate with each other.

5. Endpoint Security: Endpoints like laptops, desktops and mobile devices should be protected as they are used to access your cloud accounts.

6. Multi-Factor Authentication (MFA): Ensure MFA is enabled for each user accessing the cloud services, especially high-privileged users.

7. Cloud Access Security Broker (CASB): Implement CASB to prevent, detect or stop shadow IT and provide data loss prevention.

8. Centralized Monitoring: During and after migration, you will have security tools operating both on-premises and in the cloud. Centralizing the management and use of these tools can help your security teams identify and respond to threats and vulnerabilities more quickly and consistently. To increase your security team's effectiveness, adopt a Security Information and Event Management/ Security Operations Center (SIEM/SOC) solution.[12]

9. Secure Software Development Life Cycle: Maintaining consistency between security solutions and policy enforcement is vital, especially when they span multiple environments. Security tools should be chosen not only for their ability to operate natively in a particular cloud platform but also to integrate and operate seamlessly through the entire security policy life cycle with similar solutions deployed in different environments.[13]

10. DevSecOps: DevSecOps automates the process of securing the life cycle. It improves the security posture by baking security into every stage of the continuous delivery toolchain.

[12.] Randel, Eric, "5 Steps to Ensure Your Cloud Migration is Secure" Dec. 12, 2019 https://www.exabeam.com/how-to/5-steps-to-secure-your-cloud-migration/

[13.] Cohen, Lior, "6 Considerations for Secure Cloud Migration," Apr. 11, 2019, DevOps.com https://devops.com/6-considerations-for-secure-cloud-migration/

Post Migration

While focusing on different cloud migration challenges, it is easy to forget what will happen after the actual migration is completed. It is essential to plan the roles, responsibilities and teams of those handling the cloud infrastructure and cloud security ahead of the actual migration.

The plan should include identifying key teams and personnel responsible for monitoring the cloud platform, implementing security configurations in the future and other important functions. Processes should be appropriately reviewed and documented.

Proper access control review of the users and infrastructure should be carried out as many configurations and users might not be required once the migration is completed.

It is also beneficial to review the whole migration to learn what challenges arose during or after the migration, what can be improved in future migrations and what unplanned security dependencies were detected and remediated.

Conclusion

According to the 2020 Cloud Security Report by (ISC)2, security remains a crucial issue for cloud customers, despite the continued rapid adoption of cloud computing.[14] The report found that the vast majority of cybersecurity professionals (94%) are at least moderately concerned about public cloud security.

Unfortunately, the cloud is a great place for bad actors to conduct malicious activities and cover their tracks. Organizations need to understand the risks of moving to the cloud, the risks they can remediate and the risks they can learn to live with.

There are many critical security issues in the cloud that require a robust security solution, such as misconfiguration, identity and access management. Also, there is the challenge of limited usage visibility and a weak control plane, which can lead to data breaches and data leaks. And there is a growing concern that APIs are everywhere nowadays and are hard to secure.

Ensuring the security of your migration to the cloud depends on the type of cloud you choose, the CSP you engage with and the specific steps you take. It is essential to build security into your migration strategy, and after migrating, actively monitor your workloads to assure that your data is safe.

[14.] "2020 Cloud Security Report," Cybersecurity Insiders, (ISC)2
www.isc2.org/-/media/ISC2/Landing-Pages/2020-Cloud-Security-Report-ISC2.ashx

Additional Sources

1. "Azure compliance," webpage, Microsoft Azure
   https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance/

2. Genaev, Max, Belyaev, Aleksandr, "Security: safeguarding the back end is essential," Jun. 1, 2018, Clausematch
   https://clausematch.com/blog/safeguarding-the-back-end

3. Cook, Jeremy, "Cloud Migration Risks & Benefits," Sep. 17, 2019, Cloud Academy
   https://cloudacademy.com/blog/cloud-migration-benefits-risks/

4. Atkins, Craig, "Best practices for cloud migration amid Covid-19: From implementation to delivery," Jun. 3, 2020, CloudTech
   https://cloudcomputing-news.net/news/2020/jun/03/best-practices-for-cloud-migration-amid-covid-19-from implementation-to-delivery/

5. Das, Didyani, "Migrating to the Cloud? Here's All You Need to Know," Oct. 26, 2020, G2, https://learn.g2.com/cloud-migration

6. "How to migrate," webpage, Amazon Web Services
   https://aws.amazon.com/cloud-migration/how-to-migrate/

Capgemini engineering

About Capgemini Engineering

Capgemini Engineering combines, under one brand, a unique set of strengths from across the Capgemini Group: the world leading engineering and R&D services of Altran – acquired by Capgemini in 2020 - and Capgemini's digital manufacturing expertize. With broad industry knowledge and cutting-edge technologies in digital and software, Capgemini Engineering supports the convergence of the physical and digital worlds. We help clients unleash the potential of R&D, a key component of accelerating their journey towards Intelligent Industry. Capgemini Engineering has more than 52,000 engineer and scientist team members in over 30 countries across sectors including aeronautics, space and defense, automotive, railway, communications, energy, life sciences, semiconductors, software, and internet and consumer products.

For more details, contact us :

www.capgemini-engineering.com

Write to us at:

engineering@capgemini.com