Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2023, 10(11):85-88

Research Article ISSN: 2394 - 658X

Cloud Data Security - A Comparative Analysis of AWS, GCP, Azure Cloud Platforms

Rameshbabu Lakshmanasamy

Senior Data Engineer, Jewelers Mutual Group

ABSTRACT

Cloud Computing is becoming the primary technology companies use worldwide to facilitate storing and managing their information. The architecture gives organizations the elasticity, capacity and productivity required to manage big data. Nevertheless, as business officials vary their companies to the cloud, their data security becomes an issue. In this research article, we will discuss about the security solutions offered by three primary cloud service providers, AWS, GCP, Azure.

Keywords: Cloud, Data security, Network security, AWS, GCP, Azure, Data encryption.

Key Differences & Strengths: In this paper, we will assess cloud data security aspects by those three providers, based on data encryption, network security, security monitoring, IAM, compliance and cost. Regarding safety of creating solutions in cloud area, every platform has its advantages.

AWS has most extensive portfolio of security services and configurable options. It has been in cloud for a long time, making it preferred by many due to it's maturity. AWS Shield service is leading security solution provided by AWS, part of the AWS WAF, AWS IAM security layers. Another advantage of AWS is the ability to meet specific user's security requirements in detail as it offers most detailed level of setting configurations.

While GCP makes known its security-centered approach, hailed for its reliability, it is easily identifiable due to modern and sophisticated means of encryption, privacy AI-driven security surveillance. GCP has remarkably done well in adopting BeyondCorp, a zero-trust security model technology. This means that location does not dictate resource issues but identity and context. GCP is of great value in organizations that hold a high value of privacy and are focused on multinational regulations like GDPR.

Coming to Azure, it's core competency is its compatibility with rest of the Microsoft family. For businesses dealing with windows, Office 365 or any other Microsoft service, Azure gives offerings a smooth I&O through Azure AD. It's also beneficial in associating the enterprise-level security management of hybrid cloud; this should make Azure ideal for organizations that have both on-prem and cloud. An important feature with secration across environments includes Azure Security Center, that provides a single pane of glass to monitor security and threats.

DATA ENCRYPTION

One of the critical differentiators of cloud computing is data security since it has to be protected at rest as well as in transit. All providers provide good encryption solutions, but they differ in the ways and mechanisms they offer them.

AWS encryption is baked into its services into system architecture of AWS. Amazon S3, RDS, and EBS provide server-side encryption using best standards, such as AES-256. AWS Key Management Server and Cloud HSM (Hardware Security Module) are two services provided by Amazon to manage the encryption key safely. AWS allows customers to manage keys, but an organization can also have AWS do the key management. AWS offers SSL and TLS to protect data in transit on its network.

GCP also applies AES 256-bit encryption for data at rest, besides offering tools such as Cloud Key Management to handle the critical management. For instance, GCP also supports data encryption in transit through TLS to protect users' interaction with their cloud resources. It's encryption services are easy to use with non-impeded complete control of key management, rotation and access.

Microsoft Azure also uses AES-256 for data rest, providing customers with multiple choices for managing the enclosure. Taking its cues from AWS and GCP, Azure Key Vault offers users control of their encryption keys. It also provides Disk

Encryption for virtual machines that guarantee disk encryption for Linux and Windows systems. Data at rest and in-transit are secured by data encryption measures, such as TLS, adopted in data transfer process within services or users.

Features	AWS	Azure	GCP
Strengths	• Dominant market position • Extensive, mature offerings • Support for enterprise organizations • Global reach • Wider range of services	• Second largest provider • Integrations with Microsoft tools and software • Broad feature set • Hybrid cloud • Support for open source • Good for start-ups and developers	• Designed for cloud-native businesses • Commitment to open source and portability • Flexible contracts • DevOps expertise
Location	77 availability zones within 24 geographic regions	Presence in 60+ regions across the world	Presence in 24 regions and 73 zones. Available in 200+ countries and territories
Documentation	Best in class	High quality	High quality
Security	AWS Security Hub	Azure Security Center	Cloud Security Command Center
Compliance	AWS CloudHSM	Azure Trust Center	Google Cloud Platform Security

NETWORK SECURITY

Network Security is significant to deter intruders from gaining irresponsible access to shared resources, defend against invaders, and ensure data is safe while in transit or at rest. AWS, GCP, and Azure offer various general network security solutions, though each offers different aspects.

AWS Virtual Private Cloud (VPC) lets users create private network environments on cloud, within which users decide on a subnet and proper IP address ranges to set up specific secure communication paths. Memberships that AWS has put in place to ensure security of networks include firewalls, security groups and ACL's for traffic control. To augment this security, AWS Shield is available for protection against DDoS attacks and AWS WAF to protect web applications against threats like SQL injection and cross-site scripting.

GCP has implemented security measures based on the worldwide private fibre network. It also operates in VPC format, where, for example, Google Cloud Armor is focused on security services and DDoS protection. With Identity-Award Proxy (IAP), GCP allows organizations to affirm how users access aps to minimize risks.

Azure has similar proposition in the shape of Virtual network, or VNet for short, enabling organizations to link and safeguard their assets in individual virtual networks. While Azure offers two ways to protect against DDoS attacks, namely the DDoS Protection services, it is possible to manage and filter traffic using Network Security Groups. Another example is Azure Application Gateway, a WAF and load balancer for web applications that provides secure delivery against some threats, including DDoS attacks.

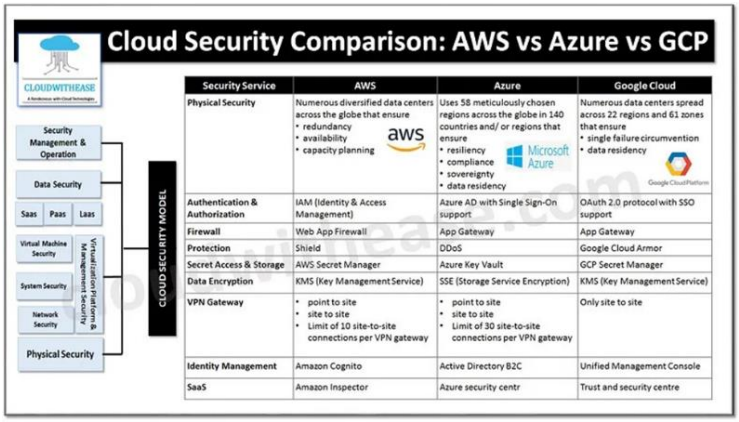
SECURITY MONITORING

Proper security monitoring is essential for an organization. It aims to identify threats, verify compliance, and respond to threats in real-time. AWS, GCP, and Aure offer complex monitoring techniques that may have different degrees of personalization and automation.

AWS currently offers several security monitoring mechanisms. CloudTrail, which records all API activity with the AWS account. This is also very beneficial in auditing and compliance jobs since it records modifications as well as the activities of users. GuardDuty is equally essential of the two services because it also employs machine learning to identify known suspicious activities including unauthorized attemps to access, etc. AI and ML algorithms to identify and alert users of patterns such as Unusual Traffic. AWS Security Hub can aggregate findings from multiple AWS services and provide high-level overview of an organization's security.

GCP provides monitoring and logging service named Stackdriver. This enables administrators to check state of the infrastructure or the application's performance being hosted on chosen infrastructure. Cloud Security Command Centre (Cloud SCC) is a security solution that can auto-detect threats, data leaks, and misconfigurations. To this end, Chronicle Security Analytics, an advanced threat detection tool, is integrated into GCP to improve its real-time capacity to deal with emerging threats.

Azure has incorporated key security monitoring from Azure Security Center, a central area of managing security in Azure. Azure Monitor is an advanced solution for monitoring telemetry data in Azure resources and tailored applications, allowing for an overall picture of the protection status to be granted. Also, the Azure Sentinel is a cloud SIEM that uses AI to identify threats, assess, and mitigate security threats.



IDENTITY AND ACCESS MANAGEMENT (IAM)

IAM is essential to cloud security because it gives organizations control over who can access their resources and what they can do with them. All three platforms, AWS, GCP, and Azure, provide strong IAM services, although they have minor differences in functionality.

AWS IAM allows the roles, users, and services of the AWS account to be controlled, consistently reviewed and proactively governed with detailed identity-based access management. AWS IAM policies specify which actions are permitted or prohibited so authorized users can only access the relevant resources (Kingsley, 2023). AWS also supports the usage of Multi-Factor Authentication (MFA), which ensures that the user has to complete another step to log in in addition to a password.

GCP's IAM system is just as comprehensive, with the capability of setting up access control at the resource level. The strategy adopted in GCP assists administrators in setting permissions at a per-resource scenario, which is more flexible and makes it easier to manage permission. The role-based access control (RBAC) that GCP provides allows the availability of access permissions across services meaning that if somebody requires different access control to somebody else, they can be given unique control to perform duties they are supposed to do or supposed to avoid.

The IAM solutions at Azure are based on the Azure Active Directory, or Azure AD, an extensive identity management solution that supports other Microsoft platforms. Azure AD provides Single sign-on (SSO), Multi-factor authentication (MFA), and conditional access policies where an admin can dictate access depending on the user's behavior or geographic location (Pluralsight, 2023). This Azure RBAC ensures that only authorized users are allowed access to Azure services, with the control granted to them limited only to what they effectively require from the services.

COMPLIANCE REQUIREMENTS

Businesses in regulated industries must meet certain security standards and legal obligations, and cloud vendors bear a great responsibility in making compliance possible. AWS, GCP, and Azure have elaborate compliance programs that assist corporate entities in meeting their compliance needs.

AWS complies with many international and industry-relevant regulations, such as GDPR, HIPAA, SOC 1/2/3, PCI-DSS, and ISO 27001. AWS Artifact includes compliance reports that can be accessed and help an organization manage its compliance processes and track compliance steps. These certifications are important to AWS as its international data centers are audited to ensure compliance constantly.

GCP is also equally compliant with other regulations, such as ISO 27001, PCI DSS, HIPAA, and GDPR. To meet these standards, Google's data centres must undergo severe auditing, and for organizations needing help with such issues, GCP features include Access Transparency and Data Loss Prevention (DLP) (Saraswat et al. 2020).

Microsoft Azure also complies with various compliances, such as GDPR, HIPAA, ISO 27001, and SOC 1/2/3. Microsoft's Azure service, available through the 'Trust Center,' offers organizations visibility of their compliance position as well as links to third-party audits. The compliance tools in Azure enable user organizations to align with compliance standards and keep valuable data secure.

COST CONSIDERATIONS

The pricing of security services differs between cloud computing service providers, such as AWS, GCP, and Azure. Investigating the security features available is one thing, but institutions must focus on getting to know the price structure within the provider's affordable spectrum.

AWS Cost: As mentioned above, the majority of AWS services are structured under the pay-as-you-go model. GuardDuty, WAF, and Shield services are available to monitor costs more than the free tier, depending on the measurement unit, such as protected resources or API calls.

GCP Cost: Of course, as with any cloud service, GCP has its price, and by today's standards, it is pretty low. In particular, when it comes to data encryption and storage, the identified platforms prefer Google Security Command Center and Cloud Armor has its pricing model in line with the number of assets to be monitored or the number of requests it needs to

handle where customers will be able to align the expenses for security solutions according to the requirements they need (Gupta & Sharma, 2023, March).

Azure Cost: Azure's pricing is also close to that of AWS; costs vary by the kind and amount of security services purchased. Pricing for Azure Security Center is based on monitored resources; tools like Azure Sentinel have a pricing model for log analytics and threat detection.

ADDITIONAL SECURITY FEATURES

In addition to the fundamental security services that a cloud provider offers, each provider provides additional services. AWS, GCP, and Azure offer products that meet particular demands and are grouped by tools.

AWS provides a service called AWS Macie that leverages machine learning to uncover, categorize, and protect the most relevant data. AWS Trusted Advisor also provides recommendations concerning the security settings within AWS environments to enhance security.

Google Cloud Platform, for instance, has BeyondCorp, which establishes a zero-trust security platform based on user identity rather than user location. This model improves security for companies with relocated, telecomm, or dispersed workforce employees.

Azure Security Center comprises a feature called Secure Score that may be used to estimate an organization's security level and identify needed changes. Secure Score also leverages compliance tools available within Azure meeting the need for organizations that require a solution to manage security and compliance.

CONCLUSION

AWS, GCP, and Azure contain vibrant and robust security solutions for those migrating to the cloud. For the security layer, AWS has many customizable security tools and granularly allows policy control. GCP provides strong encryption and features that focus on privacy. Azure has good identity management and interfaces well with the current enterprise systems. The selection criteria of cloud providers depend mainly on the security baseline, the compliance standards and the costs involved in the process. By analyzing the merits and characteristics of each platform, organizations can maintain the safety of cloud data and comply with legal and business needs.

REFERENCES

[1]. Austin, M. (2020, November 27). Microsoft Azure: The Pros and Cons. MetrixData 360. https://metrixdata360.com/cloud-series/microsoft-azure-the-pros-and-cons/

[2]. Gupta, U., & Sharma, R. (2023, March). Comparison of Different Cloud Computing Platforms for Data Analytics. In Doctoral Symposium on Computational Intelligence (pp. 67-78). Singapore: Springer Nature Singapore. https://link.springer.com/chapter/10.1007/978-981-99-3716-5_7

[3]. Kamal, M. A., Raza, H. W., Alam, M. M., & Mohd, M. (2020). Highlight the features of AWS, GCP and Microsoft Azure that have an impact when choosing a cloud service provider. Int. J. Recent Technol. Eng, 8(5), 4124-4232. https://www.researchgate.net/profile/Muhammad-Ayoub-Kamal/publication/340173446_Highlight_the_Features_of_AWS_GCP_and_Microsoft_Azure_that_Have_an_Impact_when_Choosing_a_Cloud_Service_Provider/links/5e7c397c92851caef49d994f/Highlight-the-Features-of-AWS-GCP-and-Microsoft-Azure-that-Have-an-Impact-when-Choosing-a-Cloud-Service-Provider.pdf

[4]. Kaushik , P., Rao, A. M., Singh, D. P., Vashisht, S., & Gupta, S. (2021, November). Cloud computing and comparison based on service and performance between Amazon AWS, Microsoft Azure, and Google Cloud. In 2021 International Conference on Technological Advancements and Innovations (ICTAI) (pp. 268-273). IEEE. https://ieeexplore.ieee.org/abstract/document/9673425/

[5]. Pluralsight. (2023). Cloud security comparison: AWS vs. Azure vs. GCP. Www.pluralsight.com. https://www.pluralsight.com/resources/blog/cloud/cloud-security-comparison-aws-vs-azure-vs-gcp

[6]. Prokopets, M. (2022, March 7). AWS Security vs. Azure Security: Cloud Security Comparison. Nira. https://nira.com/aws-security-vs-azure-security/

[7]. Reynolds, R. (2020, March 17). Achieving "five nines" in the cloud for justice and public safety. Amazon Web Services. https://aws.amazon.com/blogs/publicsector/achieving-five-nines-cloud-justice-public-safety/

[8]. Saraswat, M., & Tripathi, R. C. (2020, December). Cloud computing: Comparison and analysis of cloud service providers-AWs, Microsoft and Google. In 2020 9th international conference system modeling and advancement in research trends (SMART) (pp. 281-285). IEEE. https://ieeexplore.ieee.org/abstract/document/9337100/

[9]. TerryLanfear. (2021). Network security concepts and requirements in Azure. Learn.microsoft.com. https://learn.microsoft.com/en-us/azure/security/fundamentals/network-overview

[10]. Yevge, A., Ghag, P., Solanki, C., & Mishra, A. (2022). Review Paper on Cloud Service Provider–AWS, Azure, GCP. https://easychair.org/publications/preprint_download/HsX3