Cloud Security and Monitoring

What is Cloud Security? – Part 1

* Traditionally when you deploy an application, you have the entire data center, the servers that you run. You are responsible for all of it.
* In the cloud model, that is a shared responsibility between you and the cloud provider.
* In a shared responsibility model, you need to rethink security; on what your responsibility is and what the cloud provider’s responsibility is.
* When you look at PaaS, you are building applications, migrating data to the cloud, and building applications, running them on the cloud.
* You are responsible for securing the applications, the workload and the data, while the cloud provider is responsible for managing the security of the platform, so that it is compliant, it is secured from the perspective of network, the platform on down, in terms of managing the containers, the runtime and isolation.
* Whereas, if you are adopting and migrating workloads to the cloud and you are using infrastructure as a service, then the cloud provider manages the hypervisor on down. If you are using virtual servers or if you are using bare metal servers, then you can completely control everything on up, from the operating system to the virtual servers and so on.
* It is very important to understand the adoption model, whether you are consuming IaaS, or PaaS, or if you are consuming SaaS- where the club provider manages all the applications and the security of it and you worry about thee data that you bring in and plan accordingly.
* When you build applications and migrate applications or modernize you apps- let’s start with data with all the risk that you deal with and the kind of data matters.
* Is it confidential data? Is it public data or sensitive data, that may deal with private information? Consider all those factors and make a secure design around what your data security architecture should be.
* Make sure you have data at rest encryption so that the data is always encrypted, whether you use a database as a service, object store as a service or other ways to store data like block storage.
* Encryption is for amateurs.
* Key management is for professionals.
* Having more control of your keys, provide you the ability, in the context of shared responsibility model, that you own your data.
* Maybe sensitive data, you want to keep your own keys, so that how much control of the keys you have and the hardware security module in which the key processing the encryption/decryption operations happen.
* The more control you have, the more responsibility that you can take on.
* Encryption at data at rest, data in motion- as it comes from services to data stores or applications, so that as you think about data coming all the way.
* In the new world, you need to start thinking about when the application is actually processing the data, that is going to be data in this memory.
* You can start to protect data using hardware based technologies where you can protect-in-memory data as well.
* When it is in use, and in memory by the application, you can protect it.
* Take a holistic approach to data protection at rest, in motion, in use, with full control of your keys.
* It can be bring your own keys, or even better, push the boundary with keep your own keys.
* The application that serves the data- it is not only about which application needs to have access.
* Do not open up your data services to the whole world, be it network access, or everybody to access the data.
* Make sure you know exactly which applications need to access, or which users need to access the data to run your cloud applications.
* From an application viewpoint, make sure there are no vulnerabilities in your application.
* Scan your applications.
* Have an AppSec, application security, approach so that you can do dynamic scanning or static scanning of your application before you deploy it into the production.
* In the cloud native environment, you are deploying container images.
* There, you can scan your images.
* You can scan it for vulnerabilities before you deploy and set your policies so that you only have secured images in production any time.
* If there is any vulnerability in the new world, you do not need to patch these systems, you just spin up a new container and off you go.
* At a container level and the applications that serves the business logic, you can start to protect them.
* Then when you look at the users coming in, you want to manage access in terms of who the user is and from where they are coming.
* Identity- you need to make sure you know who the user is, or which service it is, based on the identity of those services or users, so that you can maintain access control to your application or data.
* Also, from the perspective of network access, you want to make sure only authorized users can get in and if there are intruders out there, you can make sure you set it up so that they are prevented from accessing you application and your data in the cloud, be it through web application firewalling, network access control or service protection.
* You need to manage access to your apps and the workload on the data that you have deployed on the cloud.

What is Cloud Security? – Part 2

* You need to have continuous security monitoring so that you know at any point whether you are compliant, your policies, you can watch out for threats that you need to manage. Having an approach and set of tools to manage security and compliance posture is very important.
* From your deployment environment, you can garner information. It can be security events, audit logs, flow logs from network or system that can be fed in so that you can figure out what your posture and complaints and threats are.
* The ability to gain visibility and insights and having that insight and turning it into actionable intelligence and remediating is very important. Let’s talk about DevOps. DevOps is about development and operations. Traditionally we think about an application team that is doing the design and architecture or building code.
* It should become Sec DevOps approach to the way you build, manage and run your applications. You need to embed security into the entire lifecycle, what we call shift left. Not only will you manage security, but shift left through the entire process. You need to have a secure design.
* As you plan, as you design and say: what kind of data am I going to put, what level of classification? What kind of applications am I building? Is it container-based? Is it a workload that I am migrating? Take that into account along with what integrations you need to do so that you plan it and architect it.
* Then you have a closed loop so that whatever you find, you may need to remediate or rearchitect your application, or implement certain things as the threats landscape evolves. In the next video, we will look at Identity and Access Management.

Cloud Encryption

* Given the concerns around data security and privacy, especially in public cloud environments, encryption plays a key role, and is often referred to as the last line of defense, in a layered security model.
* This protection not only encrypts data, but also provides robust data access control, key management, and certificate management.
* Encryption is defined as scrambling data in a way that makes it illegible. There are two parts to an encryption system- the encryption algorithm and the decryption key.
* The encryption algorithm defines the rules by which data will be transformed so that it becomes illegible and the decryption key defines how the encrypted data will be transformed back to legible data.
* Encryption ensures that only authorized users have access to sensitive data, and when accessed or intercepted without authorization, data is unreadable and meaningless.
* Cloud providers offer various cloud encryption services. This could be limited encryption of data that is identified as sensitive or end-to-end encryption of all data uploaded to the cloud.
* Data encrypted upon receipt, and encryption keys are passed to the customers to decrypt data when needed. Keys need to be managed securely.
* If you lose your keys, you will not be able to read your data.
* Data needs protection in three states- at rest, in transit, and when it is in use.
* Encryption at rest protects data while it is physically stored in a database or the storage layer. Depending on the application and business requirements, there could be multiple options for encrypting data at rest, such as encryption for block and file storage, built-in encryption in object storage, and database encryption services.
* Encryption in transit protects data while it is transmitted from one location to another. Encryption in transit includes encrypting the data before transmission, authenticating endpoints, and decrypting and verifying data on arrival.
* Secure Sockets Layer (or SSL) and Transport Layer Security (TLS) are commonly used protocols for encryption in transit. They are not only used when accessing websites securely but also for data moving between servers and services within the cloud.
* Encryption in use protects data when it is in use in memory for computations. It allows computations to be performed on encrypted text without needing to decrypt the data.
* Cloud storage encryption could be server-side or client-side. Server-side encryption occurs after cloud storage receives your data, but before the data is written to disk and stored.
* For server-side encryption you can either: Create and manage your own encryption keys, known as Customer-supplied encryption keys; or you can generate and manage your encryption keys using key management services offered by the cloud storage provider, known as Customer-managed encryption keys.
* Client-side encryption occurs before data is sent to cloud storage. This way, users can utilize encryption keys and algorithms that are not visible to the cloud provider, making it virtually impossible for cloud providers to decrypt hosted data.
* Given that a majority of enterprises today operate in multi-cloud environments, there is a need to implement a singular data protection strategy across an enterprise on-premise, hybrid, and multi-cloud deployments.
* Some cloud providers offer multi-cloud data encryption services with a range of features such as data access management, integrated key management, and sophisticated encryption that combine to deliver the scalability and flexibility to help protect the most sensitive workloads across the enterprise, regardless of where the data resides.
* Using a multi-cloud data encryption console, you can define and manage access policies, create, rotate, and manage encryption keys, and aggregate access logs.
* Encryption does not eliminate data security risk- it separates the security risk from the data itself by moving security to the encryption keys. These keys need to be managed and protected against threats in order to keep the data secure.
* Key Management Services offered by some cloud providers help perform life cycle management for encryption keys that are used in cloud services or customer-built applications.
* They enable customers to encrypt sensitive data at rest and to easily create and manage the entire lifecycle of cryptographic keys that are used to encrypt data.
* Since the keys remain in possession of the customer, the data is protected from cloud service providers.
* Some of the best practices for encryption key management include: Storing encryption keys separately from the encrypted data, taking key backups offsite and auditing them regularly, refreshing the keys periodically, and implementing multi-factor authentication for both the master and recovery keys.

Cloud Monitoring Basics and Benefits

* Cloud-based deployments can be complex.
* Monitoring performance across an entire stack of application and services can be time-consuming and draining on internal resources. This is where cloud monitoring solutions come in.
* Cloud monitoring solutions assess data, application, and infrastructure behaviors for: performance, resource allocation, network availability, compliance and security risks and threats.
* Cloud Monitoring is not just about automated tools. It includes the strategies, practices, and processes that need to be in place for analyzing, tracking, and managing cloud-based services and applications.
* It also serves to provide actionable insights that can help improve availability and user experience.
* Cloud monitoring helps to: Accelerate the diagnosis and resolution of performance incidents, control the cost of your monitoring infrastructure, mitigate the impact of abnormal situations with proactive notifications, get critical Kubernetes and container insights for dynamic microservice monitoring, and troubleshoot your applications and infrastructure.
* Cloud monitoring solutions are designed to give organizations visibility and control over their entire cloud-based infrastructure.
* They provide: Data in real-time with round the clock monitoring of virtual machines, services, databases, and applications.
* Multilayer visibility into application, user, and file access behavior across all cloud-based applications and services.
* Advanced reporting and auditing capabilities for ensuring regulatory standards are being met.
* Large-scale performance monitoring integrations across multicloud and hybrid cloud environments.
* One way to categorize cloud monitoring tools solutions is to break them down into infrastructure, Database, and Application Performance monitoring.
* Infrastructure monitoring tools help identify minor and large-scale hardware failures and security gaps so that developers and administrators can take corrective action before problems affect user experience.
* Database monitoring tools help track processes, queries, and availability of services to ensure the accuracy and reliability of database management systems.
* Application Performance Monitoring, or APM, measures application availability and performance, providing tools needed to troubleshoot insures in an application’s environment.
* APM solutions help improve user experience, meet application and user service level agreements (SLAs), minimize downtime, and lower overall operational costs.
* To get the most benefit from your cloud-based deployments, you can follow some standard cloud monitoring best practices.
* Leverage end-user experience monitoring solutions to capture the performance of an application from the point of view of its end users.
* These solutions monitor user journeys to track parameters such as application response time and frequency of use under varied conditions.
* These insights will help you to improve customer experience significantly.
* Consider moving all aspects of your infrastructure, whether in private, public, or hybrid clouds, under one unified monitoring platform. This can help you to manage all your KPIs in one place with complete visibility into performance optimization.
* Use monitoring tools that can help you track the usage and cost of your cloud resources and services.
* Increase cloud monitoring automation. This can help you gain significant operational efficiencies.
* Simulate outages and breach scenarios to evaluate how well your monitoring tools capture and alert against failures.
* Cloud monitoring needs to be a priority for organizations looking to leverage the benefits of cloud technologies.
* It will help you manage and optimize your cloud resources for cost and performance and create better customer experiences.

Lesson Summary

* Cloud security refers to the policies, technological procedures, services, and solutions designed to secure the enterprise applications and data on cloud against insider threats, data breaches, compliance issues, and organized security threats.
* Cloud security is a shared responsibility between the cloud provider and the user organization.
* Security architecture and methods for achieving continuous security need to be embedded through the life cycle of an application to ensure that the application runs on a safe platform, the code is free from vulnerabilities, and the operational risks are understood.
* Identity and Access Management, also known as access control, helps authenticate and authorize users, and provide user specific to cloud resources, services, and applications.
* As part of their Identity and Access Management services, most cloud providers offer users the ability to define access groups and create access policies that define permissions for users on account resources.
* Cloud encryption, often referred to as the last line of defense, not only encrypts data, but also provides robust data access control, key management, and certificate management.
* Data needs encryption in three states -

- Encryption at rest; protecting data while it is stored

- Encryption in transit; protecting data while it is transmitted from one location to another

- Encryption in use; protecting data when it is in use in memory

* There needs to be active monitoring of all connected systems and cloud-based services to maintain visibility of all data exchanges between public, private, and hybrid cloud environments. This ensures that the cloud provides a trusted platform that can securely integrate with your enterprise data centers.

Career Opportunities and Job Roles in Cloud Computing

* Cloud computing is a key part of an enterprise’s digital transformation strategy.
* As more and more companies are moving critical business processes and applications to a mix of cloud infrastructures, qualified cloud computing professionals are in high demand.
* According to Gartner’s report on the Cloud Services Industry, from a market size of 182.4 Billion USD in 2018 to a projected market size of 331.2 Billion USD in 2022, the market size and growth of the cloud services industry is at nearly three times the growth of overall IT services. That is the scale at which the cloud market is growing. Employer demand is outpacing the number of qualified candidates available.
* Gartner TalentNeuron’s database of more than one billion unique job listings, scores the hiring scale for jobs requiring cloud computing skills at 78, which means employers are finding it “difficult” to get the right applicants for open positions in cloud technologies.
* There are many specialization areas within this domain.
* Here is a look at some of the common roles available currently: Cloud Developers or Cloud Software Engineers, work through all phases of the software development lifecycle: writing, testing, and maintaining the code. They work with the front and back-end of applications, as well as platforms and systems that their applications run on.
* Cloud Developers need to have a mis of technical skills, business knowledge, and experience with at least one of the major cloud providers.
* Technical skill for a Cloud Developer would typically include: Knowledge of data structures, distributed systems, operating systems, and algorithms, experience with databases, proficiency in commonly used web application development languages, such as Python, JavaScript, Java, HTML, and CSS.
* Cloud Integration Specialists are responsible for integrating new cloud services, applications and infrastructure, into the organization’s portfolio of internal systems and existing cloud services.
* These specialists assess the implications and trade-offs between different solutions as they relate to the integration between external and internal systems, optimize integration and user-experience, and ensure that performance standards adhere to service level agreements set with the enterprise.
* Cloud Data Engineers are responsible for designing, developing, and deploying scalable data pipelines and data services. They look at integrating new data management technologies and software engineering tools into existing infrastructure.
* Their responsibilities include: Understanding existing systems to recommend automated integration of disparate data sets.
* Collaborating with data scientists and researchers to develop predictive models and proofs of concept.
* Promoting best practices that enable teams to accelerate their consumption and understanding of data. Improving overall efficiency by introducing new engineering processes and tools.
* Cloud Security Engineers provide expertise around the systems and processes needed to protect the confidentiality, integrity, and availability of an organization’s systems and application data. They determine security requirements, Plan, implement, and test security systems, perform threat simulations to detect possible risks. Recommend innovative technologies that will enhance the security of cloud-based environments.
* Cloud Security Engineers need to have deep knowledge of cloud platforms and services, software design patterns, and DevOps tools and methodologies.
* Cloud DevOps Engineers collaborate with development and operations teams to create reliable and rapid release pipelines for software and updates. This may typically involve: Creating custom automation tools, building an maintaining configuration and deployment frameworks, tracking design bugs and automating the debugging process for developers, maintaining and deploying web-based applications, monitoring security systems, and measuring performance against expected business outcomes.
* Containerization expertise is increasingly a must-have for DevOps Engineers.
* Cloud Solutions Architects work to translate business requirements into application architecture and design. Some of the technical skills required for a Cloud Architect role include: Deep knowledge of cloud platforms and services, deep understanding of software design patterns, knowledge of DevOps tools and methodologies, good understanding of networking, a high-level understanding of key security concepts.
* Solution Architects work closely with Cloud Developers, Networking Specialists, Security Engineers, Integration Specialists, and DevOps Engineers to architect and design solutions.
* There are several resources available for learning cloud technologies, in a variety of delivery methods, including instructor-led courses, self-paced online courses, online videos, books and technology focused community forums.
* Many cloud providers have dedicated learning portals with extensive resources available on the complete range of cloud technologies and services they provide.
* They offer learning paths, which make resources available as per specific career roles.
* Hands-on learning labs, with interactive learning resources that can be filtered by role, level, or product.
* Free trials on their suite of products and services.

Lesson Summary

* Businesses all over the world are realizing tangible benefits from the use of cloud technologies and services.
* The Weather Company migrating to the cloud to reliably deliver critical weather data at high speed, especially during major weather events such as hurricanes and tornadoes
* American Airlines using the cloud platform and technologies to deliver digital self-service tools and customer value more rapidly across its enterprise
* Cementos Pacasmayo achieving operational excellence and insight to help drive strategic transformation and reach new markets using cloud services
* Welch choosing cloud storage to drive business value from hybrid cloud
* LiquidPower using cloud-based SAP applications to fuel business growth
* The market size of the cloud services industry is at nearly three times the growth of overall IT services, escalating the need for qualified cloud computing professionals. Some of the common job roles that are available in this domain include Cloud Software Engineers, Cloud Integration Specialists, Cloud Data Engineers, Cloud Security Engineers, Cloud DevOps Engineers, and Cloud Solution Architects