Building a Robust Cloud Security Architecture for IaaS

A complete guide to proving your mettle

aspire SYSTEMS attention. always.

Chapter 1

A Deep Dive into Cloud Security

Cloud computing has become inevitable in today's business landscape and there is absolutely no shadow of doubt that it has become an integral part of a CIO's business plans. Over the last decade, the then born-in-the-cloud startups including Netflix and Spotify have brought cloud to the center stage of organizations' IT strategies. However, in order for organizations to bring the cutting edge technology at scale, prioritizing enterprise security is a step in the right direction.

A Cloud Security survey in 2020 revealed that 59% organizations expect their cloud security budget to increase over the next 12 months. Based on the data collected till date, organizations allocate approximately 27% of their security budget to cloud security.

Cloud application developers, in the recent years, have developed applications for IaaS and PaaS platforms. Although they provide basic security features such as authentication, DoS attack migration, firewall policy management, logging, basic user and profile management, security concerns continue to stall enterprise cloud adoption.

With 3 delivery models in the form of IaaS, PaaS, and SaaS and as many operational models in the form of public, private, and hybrid, the cloud security concerns and solutions are context-driven.

According to the same survey mentioned earlier, organizations have discovered the top 4 public cloud security threats: cloud platform misconfiguration (68%), unauthorized access (58%), insecure interfaces and APIs (52%), and privileged account hijacking (50%).

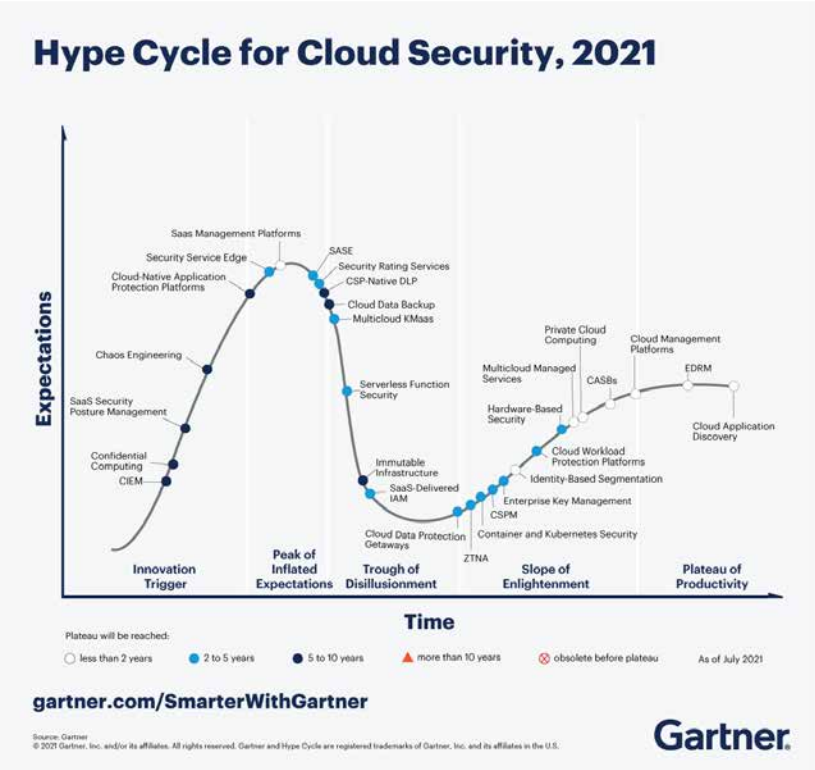
So, what can cloud architects and development teams can do in terms of architectural frameworks and tools while developing applications for IaaS and PaaS platforms?

Chapter 2

Introduction to Cloud Security Architecture

A cloud security architecture is an amalgamation of the security layers, design, and structure of the platform, tools, software, infrastructure, and best practices that exist within a cloud security solution. The architecture provides the manual to define how to configure and secure activities and operations within the cloud, including Identity and Access Management (IAM), methods to protect applications and data, and much more.

Organizations must understand its current cloud security posture, and then plan the controls and cloud security solutions used to prevent and mitigate cyber-threats. This will come handy when you plan to secure hyper-complex environments that include multiple public clouds, SaaS and PaaS services, on-premise resources among others. These public clouds are accessed from both corporate and unsecured personal devices.

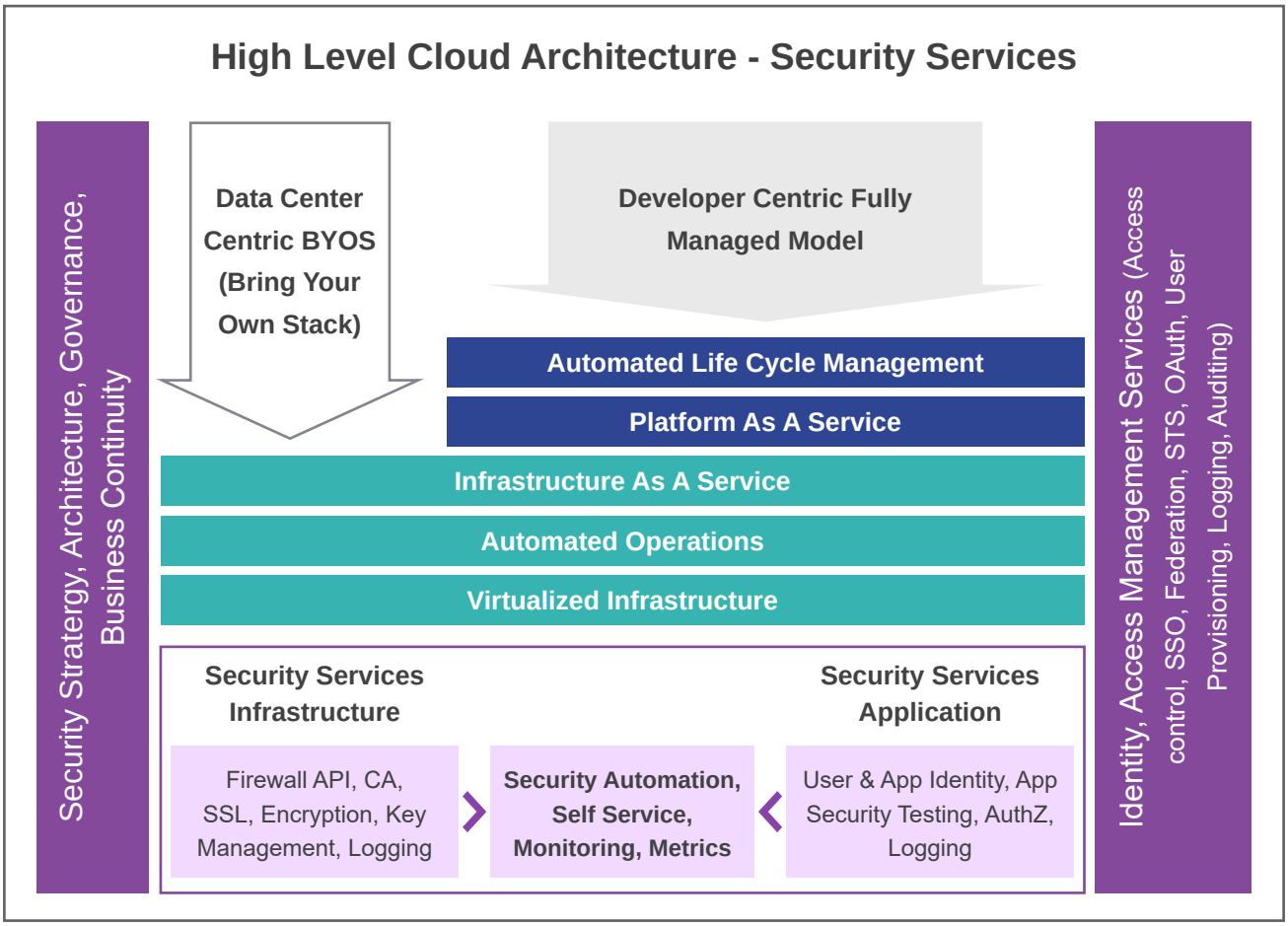


Need for a Cloud Security Architecture

While the number of organizations that have taken the cloud route has multiplied drastically, they are also keen on ensuring enterprise security. Although majority of the off-network data passes through cloud-based services, many of these cloud services are functioning without any security.

CSPs and multiple personal devices make it a challenge for organizations to get a holistic view of data flows. Cloud collaboration exceeds traditional network control measures and access to sensitive data on personal devices poses a major threat.

Security and malware experts find it challenging to monitor a complex mix of personal and corporate devices, networks, and clouds. These gaps in network security are an invitation for attackers to breach the system.



Not many cloud service providers offer detailed information on their internal cloud environment, and their common internal security controls cannot be directly transferred to a public cloud.

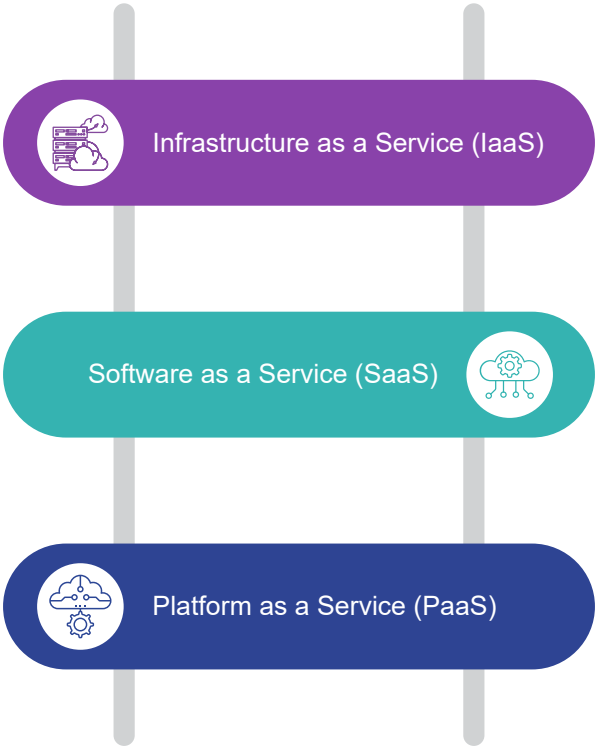
Henceforth, organizations must think about having cloud security architecture at the center of their cloud environment.

Chapter 3

Types of Cloud Security Architecture

Implementing cloud security architecture solely depends on the type of cloud model your organizations has chosen. Once you choose the cloud model you desire, you need to consider your security architecture as the guiding principle of what you need to configure, deploy, and manage for your environment's best security.

Since each of these cloud models has shared responsibilities with the cloud provider, it is wise to understand which models you have implemented to be aware of your security responsibilities. The current 3 primary styles are:



The 3 cloud offerings give the luxury of providing a cloud-native architecture to the customers for running applications and services from outside the organization. A cloud-native architecture essentially allows an application or a service to be designed exclusively for the cloud. Going cloud-native is a decision you need to take during the inception stages of the project.

Chapter 4

Key Elements of Cloud Security Architecture

If you go for a cloud-native environment from your cloud provider, the security aspects are provided to whoever is providing the cloud services. Listed below are some of the key elements to remember while designing cloud infrastructure:

- **Security at each layer:** Ensuring that every layer of your cloud security architecture is self-defending is paramount. With multiple components available in each layer, automatic updates on operating systems, secure coding, and monitoring logs come in very handy.
- **Centralized management of components:** Managing multiple components in each layer, including security, from a single repository calls for better efficiency.
- **Design for Redundancy in case of failures:** Although we remain optimistic about the fact that the cloud security architecture is end-to-end secured, there's always room for failure or mishap. Businesses need to ensure they have chalked out disaster recovery plans and having back-ups on hand to resume operations. Resilience is the key to achieving this.
- **Design for Elasticity and Scalability:** With respect to elasticity, you need to figure out specific design options. When scaling, are you willing to expand the server or add more services? What is the maximum threshold that dictates when to scale up and down? Businesses need to find answers to these questions before they build the security architecture.
- **Choose the right storage for your deployments:** While choosing storage, choose a repository which suits your organization's use cases and needs. Time should not be a constraint while exploring the options since they aren't created equal. Each has a unique set of security controls and performance specifications. This is the right time to revisit data security strategies and make sure you are complying with company's guidelines.
- **Plan for Alerts and Notifications:** While designing how the components communicate with each other and how users communicate with those components, you need to make sure you're alerted and notified. This helps you keep track of what's happening in your cloud infrastructure. With your primary source of information being the logs created, it is wise to enable logging wherever you can.
- **Centralization, Standardization, & Automation:** Centralization is using services and tools that can be brought into a single repository for viewing. Standardization is creating consistent cloud architecture security models across all your services offered in the cloud, thereby limiting the burden of implementation. Automation – the more you automate your infrastructure, the quicker you can scale up and fix issues.

Chapter 5

Shared Responsibilities of Cloud Security

With cloud architectures moving towards the serverless approach and living in a shared environment, it's time to remove the use of standard security tools that organizations have been using so far. This is because standard tools are not designed to run in containers. With the standard security tools becoming obsolete, there is more reliance on CASB, Zero Trust, and CWPP.

Cloud security architecture is an instrumental part of your IT infrastructure. The concept of integrating security into the infrastructure allows you to manage, expand, and monitor the cloud environment. Failure to implement security leads to security incidents, leading to loss of data.

Shared Responsibility Model for security in the Cloud

On-Premises (for reference)	IaaS (infrastructure-as-a-service)	PaaS (Platform-as-a-service)	SaaS (software-as-aservice)
User Access	**User Access**	**User Access**	**User Access**
Data	**Data**	**Data**	**Data**
Applications	**Applications**	**Applications**	Applications
Operating System	**Operating System**	Operating System	Operating System
Network Traffic	**Network Traffic**	Network Traffic	Network Traffic
Hypervisor	Hypervisor	Hypervisor	Hypervisor
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical

Customer Responsibility | Cloud Provider Responsibility

Public Cloud vs Private Cloud

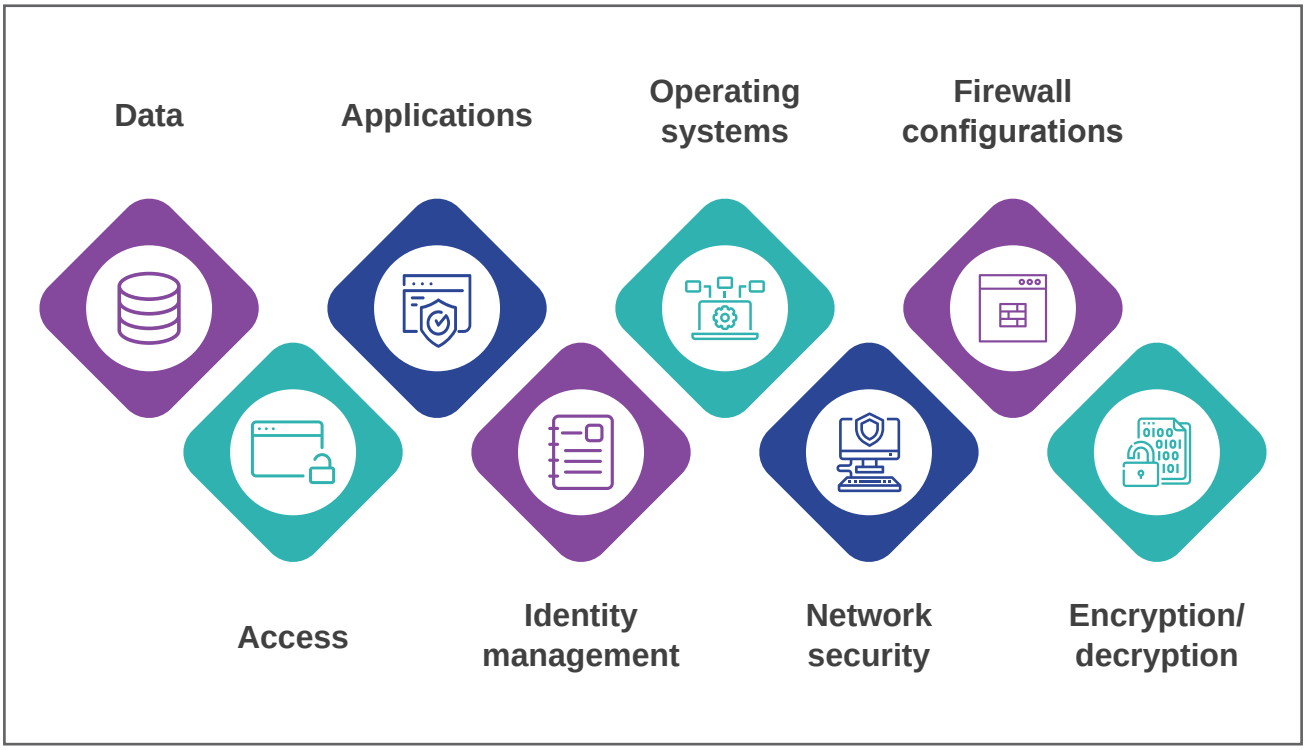
The public cloud is where organizations use a cloud service provider with shared resources and compute among multiple customers. The data and access are unique and hidden from each customer and each customer is sharing a rented space within the cloud. In this model, the customer and the cloud service provider share equal responsibilities for security.

The private cloud, on the other hand, is infrastructure owned by the organization using it, and can be onsite in a data center or hosted on-premise. In this model, almost everything is customer's responsibility.

Provider vs Consumer Responsibilities

With cloud hosting service providers, the responsibility lies in the security of the cloud. In simple terms, they are responsible for the software (compute, storage, database etc.) and the hardware or infrastructure security.

For customer of cloud providers, their sole responsibility is the security in the cloud that includes:



According to Gartner, through 2023, a minimum of 99% cloud security failures will be the customer's fault.

This isn't surprising considering the huge amounts of responsibility and the significant shift for organizations to migrate to a cloud model.

Chapter 6

IaaS Cloud Security Architecture

IaaS is a cloud model where organizations can purchase infrastructure from a cloud provider. With the systems and networks easily built, organizations can install their own operating systems, applications, and middleware. Examples of IaaS include AWS and Azure.

The security threats for the IaaS cloud model are similar to that of the on-premise threats. As mentioned earlier, since organizations install their own OS and applications, they are also responsible for the security that carries with it.

With possible recurring threats including vulnerabilities, malware, insider threats, and credential exposure, you will want to have standard security tools along with cloud-specific tools such as Endpoint Protection (EPP), CASBs, and vulnerability management. You can also implement these tools in access management, data encryption, and network encryption. Implementing both standard security tools and cloud-specific tools will account for a better security strategy by creating layers of security.

Gartner predicts that 50% of enterprises will have accidentally exposed some IaaS storage services, network segments, and applications directly to the public internet.

Chapter 7

What's an Ideal Cloud Security Maturity Model?

The cloud security maturity model (CSMM) entails a set of guidelines that may or may not comply with every organization. These guidelines will help you make better investment decisions into specific areas of your cloud environment.

With different maturity models from various organizations, it's important to choose the one that suits your business requirements. Listed below are the things to look for from your cloud service provider:

- Do you have the luxury of multi-factor authentication methods?
- Do they allow for Single Sign On (SSO) access?
- Do you integrate with enterprise authentication?

Businesses should look into the cloud service provider's past to evaluate how they've handled security incidents.

Examples: How many breaches have they experienced? Have they hosted malware in their cloud? Are regular penetration tests performed?

Policies, compliance information and documents also need to be taken into consideration. If you find out how your cloud service provider handles their security, it gives you a fair idea about how they'll handle yours. Do they notify you whenever a security breach occurs?

Leave no stones unturned while evaluating your cloud service provider. The sanctity of your organization's security is not to be taken lightly and you want to be fully informed while making critical decisions.

Chapter 8

Tips for Building Your Cloud Security Architecture

1. Conduct Due Diligence

Before migrating to the cloud, businesses must carefully investigate the security and resilience properties of the cloud provider as a whole and their multitude of services.

The due diligence process consists of:

- Defining security and availability benchmarks based on previous data from organizations
- Investigating your cloud provider's security best practices and their impact on your business
- Exploring your cloud provider's security capabilities such as encryption, logging, and identity and access management (IAM)
- Understanding how your cloud provider can comply with your business standards
- Learning the specifics of the shared responsibility model for your cloud provider
- Evaluating first-party security services offered by the cloud provider
- Check if existing security tools are relevant for your new cloud environment

2. Determine which data is the most sensitive

It's not feasible to apply stringent security measures for your data, irrespective of the size of the organization. Some data shall remain unsecured, but the onus is on the organization to decide which data categories must be protected and which ones shall remain as such.

Businesses leverage automated data classification engines to decide which data categories must be secured from breaches. These engines are determined to find sensitive data across networks, endpoints, databases, and the cloud, allowing organizations to identify the data categories to enhance security.

3. Bring Employee Cloud Usage out of the shadows

Implementing a corporate cloud security strategy doesn't mean your employees must abide by it. Employees seldom consult with the IT department before accessing the common cloud services.
The shadow use of the cloud can be measured by an organization's web proxy, firewall, and SIEM logs. These will provide a holistic view of the services used by the employees on a regular basis. Another important aspect of shadow usage is the access to legitimate cloud resources from personal devices. Access to any cloud service from personal devices creates a gap in cloud security.

4. Protect Cloud Endpoints

Several organizations are implementing endpoint protection platforms with multi-layered protection including endpoint detection and response (EDR), next-generation antivirus (NGAV), and user and entity behavior analysis (UEBA).
Endpoint protection plays a crucial role in the cloud as they compute instances, storage volumes and buckets, and managed services like Amazon RDS. These tools also help organizations in controlling the cloud workloads and protect the weakest links in the cloud with enhanced security.

5. Understanding your role in compliance

Regulatory compliance is your business' sole responsibility. Irrespective of how many business functions you move to the cloud, the onus is on you to select a cloud architecture platform that will comply with all the regulatory standards. (Ex: PCI DSS, GDPR, HIPAA, CCPA).
Assess the tools and services offered by your cloud provider to ensure compliance and decipher which third-party tools you can use to create cloud systems.

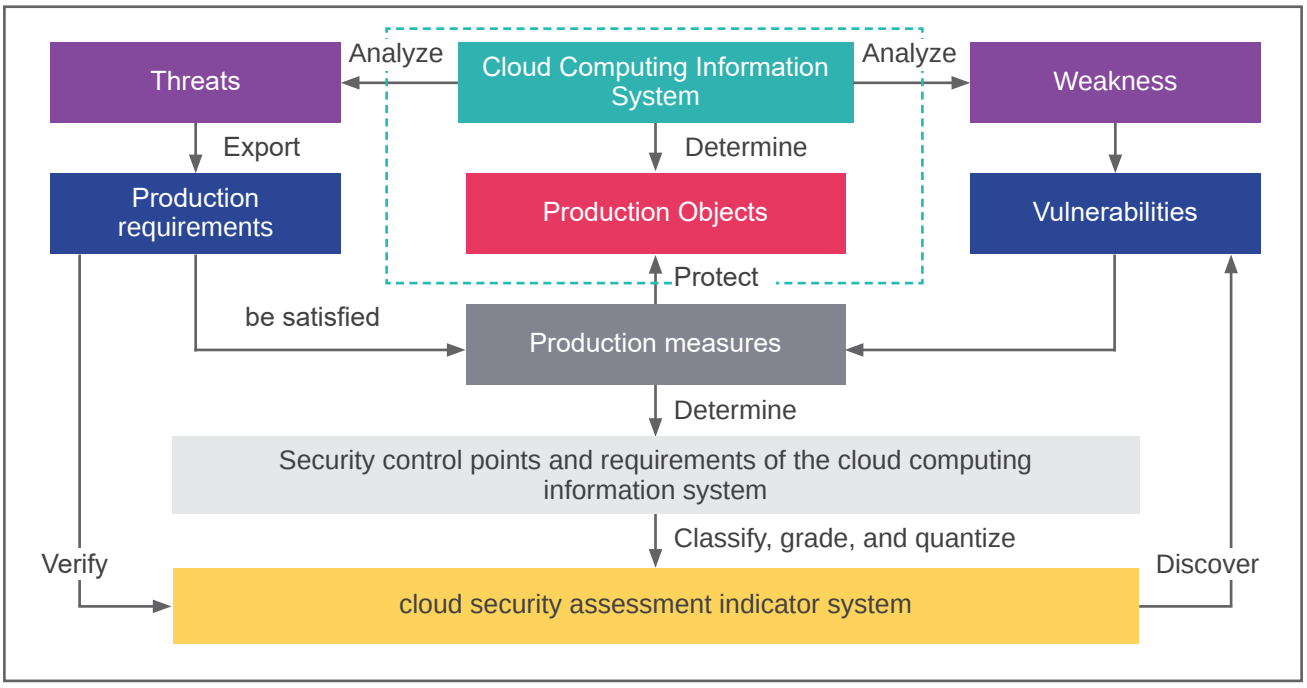
Chapter 9

Cloud Security Assessment

A cloud security assessment evaluates an organization's cloud infrastructure to ensure the organization is end-to-end secured. In order to identify weaknesses and potential points of entry into the cloud infrastructure, the cloud security assessment helps in analyzing the network for evidence of exploitation and chalk out strategies to prevent attacks in the future.

An ideal cloud security assessment focuses on improving the following 7 aspects:

- **Overall security posture**
- **Access control and management**
- **Network security**
- **Incident management**
- **Storage security**
- **Platform services security**
- **Workload security**

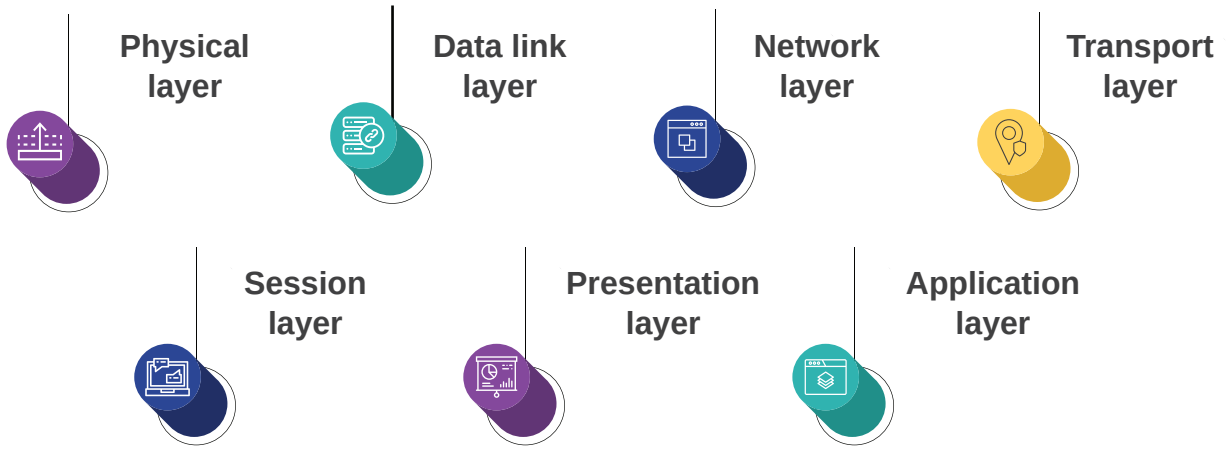


While organizations are having multiple cloud accounts or subscriptions with varying levels of security, the impact of a breach can have serious effects in cloud environments. Unlike a traditional network with a perimeter security model, the cloud environment requires advanced security measures.

The alarming issue in cloud security is misconfiguration. The root cause of security breaches, cloud misconfigurations is the blips made by network engineers when the cloud was in its infancy. A cloud security assessment addresses these concerns including any outdated aspects in the security model.

Excessive network permissions to untrusted third parties through inbound traffic also play a significant role. Lack of multi-factor authentication (MFA) and improper logging make malicious activities more challenging to detect, characterize, and recover.

The Open Systems Interconnection or the OSI Model sets out recommendations for application security in each of the 7 layers in your cloud environment. The 7 layers are:



Reach out to us for a free demo to get your cloud environment assessed by our cloud experts.

Chapter 10

Conclusion

Building cloud security architecture is not a cakewalk. The time is ripe to address your business' security policies, relevant compliance standards, and security best practices for your cloud environment. The 5 tips listed above will make your cloud security architecture a grand success.

At Aspire, our team of cloud experts will help you construct a robust, effective cloud security strategy for your organization.

aspire SYSTEMS
attention. always.

About **Aspire Systems**

- Global technology services firm with core DNA of Software Engineering
- Specific areas of expertise around Software Engineering, Digital Services,
- Testing, and Infrastructure & Application Support
- The vertical focus among Independent Software Vendors, Retail, Distribution &
- Consumer Products and BFSI
- 3000+ employees; 150+ active customers
- Oracle Global Platinum Partnership with OCI & R12.2.9, Domain Expertise
- Well Rounded Team covering Cloud Architects, Solution Experts & Application
- Consultants
- CMMI Maturity Level 3, ISO 9001:2015, and ISO 27001: 2013 certified
- International headquarters in Singapore with presence across US, Mexico, UK,
- The Netherlands, Poland, Middle East, and India
- Recognized 11 consecutive times as “Best Place to Work for” by GPW Institute

Contact Us

For more info contact: **info@aspiresys.com** or visit **www.aspiresys.com**

NORTH AMERICA	POLAND	INDIA	MIDDLE EAST
+1 630 368 0970	+48 58 732 77 71	+91 44 6740 4000	+971 50 658 8831

NETHERLANDS	UNITED KINGDOM	SINGAPORE	MEXICO
+31 (0)30 800 92 16	+44 203 170 6115	+65 3163 3050	+52 222 980 0115