It is a set of control-based technologies & policies adapted to stick to regulatory compliances, rules & protect data application and cloud technology infrastructure. Because of cloud's nature of sharing resources, cloud security gives particular concern to identity management, privacy & access control. So the data in the cloud should have to be stored in an encrypted form. With the increase in the number of organizations using cloud technology for a data operation, proper security and other potentially vulnerable areas became a priority for organizations contracting with cloud providers. Cloud computing security processes the security control in cloud & provides customer data security, privacy & compliance with necessary regulations.

Security Planning for Cloud

Before using cloud technology, users should need to analyze several aspects.

These are:

- Analyze the sensitivity to risks of user's resources.
- The cloud service models require the customer to be responsible for security at various levels of service.
- Understand the data storage and transfer mechanism provided by the cloud service provider.
- Consider proper cloud type to be used.

Cloud Security Controls

Cloud security becomes effective only if the defensive implementation remains strong.

There are many types of control for cloud security architecture; the categories are listed below:

1. **Detective Control**: are meant to detect and react instantly & appropriately to any incident.
2. **Preventive Control**: strengthen the system against any incident or attack by actually eliminating the vulnerabilities.
3. **Deterrent Control** is meant to reduce attack on cloud system; it reduces the threat level by giving a warning sign.
4. **Corrective Control** reduces the consequences of an incident by controlling/limiting the damage. Restoring system backup is an example of such type.

Understanding The Data Security

As we all know the data is transferred via the internet, so one of the major concerns is data security. The major points that one should adopt to secure cloud data are:

- Access Control
- Auditing

- Authentication
- Authorization

CSA (Cloud Security Alliance) MODEL

This stack model defines the boundaries of each service model & shows with how much variation the functional units relate to each other. It is responsible for creating the boundary between the service provider & the customer.

CSA Model's Key Points:

- IaaS is the most basic level among all services.
- Each of the services inherits the capabilities and security concerns of the model beneath.
- The infrastructure, platform for development & software operating environment are provided by IaaS, PaaS & SaaS respectively.
- The security mechanism below the security boundary must be built into the system that is required to be maintained by the customer.

Encrypt Cloud Data:

Encryption protects data from being compromised. It helps in protecting data that is being transferred & stored in the cloud. Encryption helps both protect unauthorized access along with the prevention of data loss.

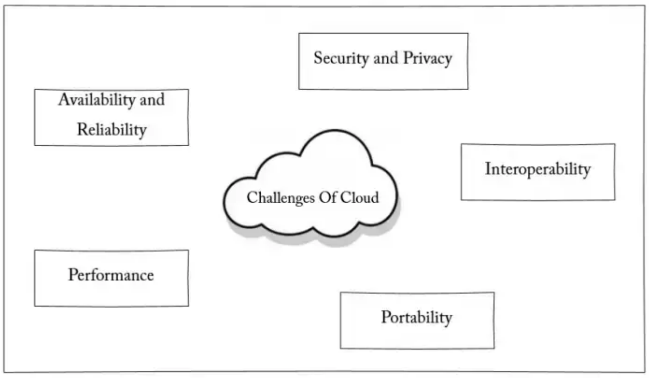
Challenges of Cloud Computing

This emergent cloud technology is facing many technological challenges in different aspects of data & information handling & storage.

Some of the challenges are as follows:

- Availability & reliability
- Security & Privacy
- Interoperability
- Performance
- Portability

Figure - Challenges Of Cloud:



The challenges as mentioned above are the most important and concerned points that should be processed for the betterment.

CLOUD SECURITY ISSUES:
RISKS, THREATS, AND CHALLENGES

All companies face security risks, threats, and challenges every day. Many think these terms all mean the same thing, but they're more nuanced. Understanding the subtle differences between them will help you better protect your cloud assets.

What is the difference between risks, threats, and challenges?

- A **risk** is a potential for loss of data or a weak spot.
- A **threat** is a type of attack or adversary.
- A **challenge** is an organization's hurdles in implementing practical cloud security.

Let's consider an example: An API endpoint hosted in the cloud and exposed to the public Internet is a **risk**, the attacker who tries to access sensitive data using that API is the **threat** (along with any specific techniques they could try), and your organization's **challenge** is effectively protecting public APIs while keeping them available for legitimate users or customers who need them.

A complete cloud security strategy addresses all three aspects, so no cracks exist within the foundation. You can think of each as a different lens or angle with which to view cloud security. A solid strategy must mitigate risk (security controls), defend against threats (secure coding and deployment), and overcome challenges (implement cultural and technical solutions) for your business to use the cloud to grow securely.

4 Cloud Security Risks

You cannot completely eliminate risk; you can only manage it. Knowing common risks ahead of time will prepare you to deal with them within your environment. **What are four cloud security risks?**

1. Unmanaged Attack Surface
2. Human Error
3. Misconfiguration
4. Data Breach

1. Unmanaged Attack Surface

An attack surface is your environment's total exposure. The adoption of microservices can lead to an explosion of publicly available workload. Every workload adds to the attack surface. Without close management, you could expose your infrastructure in ways you don't know until an attack occurs.

Attack surface can also include subtle information leaks that lead to an attack. For example, CrowdStrike's team of threat hunters found an attacker using sampled DNS request data gathered over public WiFi to work out the names of S3 buckets. CrowdStrike stopped the attack before the attackers did any damage, but it's a great illustration of risk's ubiquitous nature. Even strong controls on the S3 buckets weren't enough to completely hide their existence. As long as you use the public Internet or cloud, you're automatically exposing an attack surface to the world.

Your business may need it to operate, but keep an eye on it.

2. Human Error

According to Gartner, through 2025, 99% of all cloud security failures will be due to some level of human error. Human error is a constant risk when building business applications. However, hosting resources on the public cloud magnifies the risk.

The cloud's ease of use means that users could be using APIs you're not aware of without proper controls and opening up holes in your perimeter. Manage human error by building strong controls to help people make the right decisions.

One final rule — don't blame people for errors. Blame the process. Build processes and guardrails to help people do the right thing. Pointing fingers doesn't help your business become more secure.

3. Misconfiguration

Cloud settings keep growing as providers add more services over time. Many companies are using more than one provider.

Providers have different default configurations, with each service having its distinct implementations and nuances. Until organizations become proficient at securing their various cloud services, adversaries will continue to exploit misconfigurations.

4. Data Breaches

A data breach occurs when sensitive information leaves your possession without your knowledge or permission. Data is worth more to attackers than anything else, making it the goal of most attacks. Cloud misconfiguration and lack of runtime protection can leave it wide open for thieves to steal.

The impact of data breaches depends on the type of data stolen. Thieves sell personally identifiable information (PII) and personal health information (PHI) on the dark web to those who want to steal identities or use the information in phishing emails.

Other sensitive information, such as internal documents or emails, could be used to damage a company's reputation or sabotage its stock price. No matter the reason for stealing the data, breaches continue to be an imposing threat to companies using the cloud.

How To Manage Cloud Security Risks

Follow these tips to manage risk in the cloud:

- Perform regular risk assessments to find new risks.
- Prioritize and implement security controls to mitigate the risks you've identified (CrowdStrike can help).
- Document and revisit any risks you choose to accept.

4 Cloud Security Threats

A threat is an attack against your cloud assets that tries to exploit a risk. **What are four common threats faced by cloud security?**

1. Zero-Day Exploits
2. Advanced Persistent Threats
3. Insider Threats
4. Cyberattacks

1. Zero-day Exploits

Cloud is "someone else's computer." But as long as you're using computers and software, even those run in another organization's data center, you'll encounter the threat of zero-day exploits.

Zero-day exploits target vulnerabilities in popular software and operating systems that the vendor hasn't patched. They're dangerous because even if your cloud configuration is top-notch, an attacker can exploit zero-day vulnerabilities to gain a foothold within the environment.

2. Advanced Persistent Threats

An advanced persistent threat (APT) is a sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network to steal sensitive data over a prolonged time.

APTs aren't a quick "drive-by" attack. The attacker stays within the environment, moving from workload to workload, searching for sensitive information to steal and sell to the highest bidder. These attacks are dangerous because they may start using a zero-day exploit and then go undetected for months.

3. Insider Threats

An insider threat is a cybersecurity threat that comes from within the organization — usually by a current or former employee or other person who has direct access to the company network, sensitive data and intellectual property (IP), as well as knowledge of business processes, company policies or other information that would help carry out such an attack.

4. Cyberattacks

A cyber attack is an attempt by cybercriminals, hackers or other digital adversaries to access a computer network or system, usually for the purpose of altering, stealing, destroying or exposing information.

Common cyberattacks performed on companies include malware, phishing, DoS and DDoS, SQL Injections, and IoT based attacks.

As companies increase their use of cloud hosting for storage and computing, so increases the risk of attack on their cloud services. Proactive prevention is always preferred over required remediation.**Read more about cloud specific vulnerabilities and how to prevent them**

How to Handle Cloud Security Threats

There are so many specific attacks; it's a challenge to protect against them all. But here are three guidelines to use when protecting your cloud assets from these threats and others.

- Follow secure coding standards when building microservices
- Double and triple check your cloud configuration to plug any holes
- With a secure foundation, go on the offensive with threat hunting. (CrowdStrike can help)

4 Cloud Security Challenges

Challenges are the gap between theory and practice. It's great to know you need a cloud security strategy. But where do you start? How do you tackle cultural change? What are the daily practical steps to make it happen?

What are four cloud security challenges every company faces when embracing the cloud?

1. Lack of Cloud Security and Skills
2. Identity and Access Management
3. Shadow IT
4. Cloud Compliance

1. Lack Of Cloud Security Strategy and Skills

Traditional data center security models are not suitable for the cloud. Administrators must learn new strategies and skills specific to cloud computing.

Cloud may give organizations agility, but it can also open up vulnerabilities for organizations that lack the internal knowledge and skills to understand security challenges in the cloud effectively. Poor planning can manifest itself in misunderstanding the implications of the shared responsibility model, which lays out the security duties of the cloud provider and the user. This misunderstanding could lead to the exploitation of unintentional security holes.

2. Identity and Access Management

Identity and Access Management (IAM) is essential. While this may seem obvious, the challenge lies in the details.

It's a daunting task to create the necessary roles and permissions for an enterprise of thousands of employees. There are three steps to a holistic IAM strategy: role design, privileged access management, and implementation.

Begin with a solid role design based on the needs of those using the cloud. Design the roles outside of any specific IAM system. These roles describe the work your employees do, which won't change between cloud providers.

Next, a strategy for privileged access management (PAM) outlines which roles require more protection due to their privileges. Tightly control who has access to privileged credentials and rotate them regularly.

Finally, it's time to implement the designed roles within the cloud provider's IAM service. This step will be much easier after developing these ahead of time.

3. Shadow IT

Shadow IT challenges security because it circumvents the standard IT approval and management process.

Shadow IT is the result of employees adopting cloud services to do their jobs. The ease with which cloud resources can be spun up and down makes controlling its growth difficult. For example, developers can quickly spawn workloads using their accounts. Unfortunately, assets created in this way may not be adequately secured and accessible via default passwords and misconfigurations.

The adoption of DevOps complicates matters. Cloud and DevOps teams like to run fast and without friction. However, obtaining the visibility and management levels that the security teams require is difficult without hampering DevOps activities. DevOps needs a frictionless way to deploy secure applications and directly integrate with their continuous integration/continuous delivery (CI/CD) pipeline. There needs to be a unified approach for security teams to get the information they need without slowing down DevOps. IT and security need to find solutions that will work for the cloud — at DevOps' velocity.

4. Cloud Compliance

Organizations have to adhere to regulations that protect sensitive data like PCI DSS and HIPAA. Sensitive data includes credit card information, healthcare patient records, etc. To ensure compliance standards are met, many organizations limit access and what users can do when granted access. If access control measures are not set in place, it becomes a challenge to monitor access to the network.

How to Overcome Cloud Security Challenges

Each challenge is different and therefore requires unique solutions. Take the time to plan before making use of any cloud services. A sound strategy takes into consideration any common cloud challenges like the ones we've discussed here. Then you'll have a plan of action for each anticipated challenge.