Unit-5

Cloud Security

Cloud security refers to the technologies, policies, controls, and services that protect cloud data, applications, and infrastructure from threats.

Most cloud providers attempt to create a secure cloud for customers. Their business model hinges on preventing breaches and maintaining public and customer trust. Cloud providers can attempt to avoid cloud security issues with the service they provide, but can't control how customers use the service, what data they add to it, and who has access. Customers can weaken cybersecurity in cloud with their configuration, sensitive data, and access policies. In each public cloud service type, the cloud provider and cloud customer share different levels of responsibility for security. By service type, these are:

- **Software-as-a-service (SaaS)** — Customers are responsible for securing their data and user access.
- **Platform-as-a-service (PaaS)** — Customers are responsible for securing their data, user access, and applications.
- **Infrastructure-as-a-service (IaaS)** — Customers are responsible for securing their data, user access, applications, operating systems, and virtual network traffic.

Cloud security challenges

Since data in the public cloud is being stored by a third party and accessed over the internet, several challenges arise in the ability to maintain a secure cloud. These are:

- Visibility into cloud data — In many cases, cloud services are accessed outside of the corporate network and from devices not managed by IT. This means that the IT team needs the ability to see into the cloud service itself to have full visibility over data, as opposed to traditional means of monitoring network traffic.
- Control over cloud data — In a third-party cloud service provider's environment, IT teams have less access to data than when they controlled servers and applications on their own premises. Cloud customers are given limited control by default, and access to underlying physical infrastructure is unavailable.
- Access to cloud data and applications —Users may access cloud applications and data over the internet, making access controls based on the traditional data center network perimeter no longer effective. User access can be from any location or device, including bring-your-own-device (BYOD) technology. In addition, privileged access by cloud provider personnel could bypass your own security controls.
- Compliance — Use of cloud computing services adds another dimension to regulatory and internal compliance. Your cloud environment may need to adhere to regulatory requirements such as HIPAA, PCI and Sarbanes-Oxley, as well as requirements from internal teams, partners and customers. Cloud provider infrastructure, as well as interfaces between in-house systems and the cloud are also included in compliance and risk management processes.
- Cloud-native breaches – Data breaches in the cloud are unlike on-premises breaches, in that data theft often occurs using native functions of the cloud. A Cloud-native breach is a series of actions by an adversarial actor in which they "land" their attack by

exploiting errors or vulnerabilities in a cloud deployment without using malware, "expand" their access through weakly configured or protected interfaces to locate valuable data, and "exfiltrate" that data to their own storage location.

- Misconfiguration – Cloud-native breaches often fall to a cloud customer's responsibility for security, which includes the configuration of the cloud service. Research shows that just 26% of companies can currently audit their IaaS environments for configuration errors. Misconfiguration of IaaS often acts as the front door to a Cloud-native breach, allowing the attacker to successfully land and then move on to expand and exfiltrate data. Research also shows 99% of misconfigurations go unnoticed in IaaS by cloud customers. Here's an excerpt from this study showing this level of misconfiguration disconnect.
- Disaster recovery – Cybersecurity planning is needed to protect the effects of significant negative breaches. A disaster recovery plan includes policies, procedures, and tools designed to enable the recovery of data and allow an organization to continue operations and business.
- Insider threats – A rogue employee is capable of using cloud services to expose an organization to a cybersecurity breach. A recent McAfee Cloud Adoption and Risk Report revealed irregular activity indicative of insider threat in 85% of organizations.

Cloud Security risks

1. **Theft or loss of intellectual property**
   An outstanding 21% of data uploaded by companies to cloud-based file management services contain sensitive data. The analysis that was done by Skyhigh found that companies face the risk of having their intellectual property stolen. Employees unwittingly help cyber-criminals access sensitive data stored in their cloud accounts.

   Weak cloud security measures within an organization include storing data without encryption or failing to install multi-factor authentication to gain access to the service.

2. **Compliance violations**
   Organizations can quickly go into a state of non-compliance, which puts them in the risk of serious consequences.
   Even tech giants like Facebook have been victims of resource exploitation due to user error or misconfigurations. Keeping employees informed about the dangers and risks of data sharing is of at most importance.
3. **Malware attacks**
   Cloud services can be a vector for data exfiltration. As technology improves, and protection systems evolve, cyber-criminals have also come up with new techniques to deliver malware targets. Attackers encode sensitive data onto video files and upload them to YouTube.

   Skyhigh reports that cyber-criminals use private twitter accounts to deliver the malware. The malware then exhilarates sensitive data a few characters at a time. Some have also been known to use phishing attacks through file-sharing services to deliver the malware.

4. **End-user control**
   When a firm is unaware of the risk posed by workers using cloud services, the employees could be sharing just about anything without raising eyebrows. Insider threats have

become common in the modern market. For instance, if a salesman is about to resign from one firm to join a competitor firm, they could upload customer contacts to cloud storage services and access them later.

The example above is only one of the more common insider threats today. Many more risks are involved with exposing private data to public servers.

5. **Contract breaches with clients and/or business partners**

   Contracts restrict how business partners or clients use data and also who has the authorization to access it. Employees put both the firm and themselves at risk of legal action when they move restricted data into their cloud accounts without permission from the relevant authorities.

   Violation of business contracts through breaching confidentiality agreements is common. This is especially when the cloud service maintains the right to share all data uploaded with third parties.

6. **Shared vulnerabilities**

   Cloud security is the responsibility of all concerned parties in a business agreement. From the service provider to the client and business partners, every stakeholder shares responsibility in securing data. Every client should be inclined to take precautionary measures to protect their sensitive data.

   While the major providers have already taken steps to secure their side, the more delicate control measures are for the client to take care of. Dropbox, Microsoft, Box, and Google, among many others, have adopted standardized procedures to secure your data. These measures can only be successful when you have also taken steps to secure your sensitive data.

   Key security protocols such as protection of user passwords and access restrictions are the client's responsibility. According to an article named "Office 365 Security and Share Responsibility" by Skyfence, users should consider high measures of security as the most delicate part of securing their data is firmly in their hands.

7. **Attacks to deny service to legitimate users**

   You are most likely well aware of cyber-attacks and how they can be used to hijack information and establish a foothold on the service provider's platform. Denial of service attacks, unlike cyber-attacks, do not attempt to bypass your security protocol. Instead, they make your servers unavailable to illegitimate users.

   However, in some cases, DoS is used as a smokescreen for a variety of other malicious activities. They can also be used to take down some security appliances like web application firewalls.

8. **Insecure APIs**

   API or Application Programming Interfaces offer users the opportunity to customize their cloud service experience. APIs can, however, be a threat to cloud security due to their very nature. Apart from giving firms the ability to customize the features on their cloud service provider, they also provide access, authenticate, and effect encryption.

   As APIs evolve to provide better service to users, they also increase their security risk on the data client's store. APIs provide programmers with the tools to integrate their programs with job-critical applications. YouTube is one of the sites with an API that allows users to embed YouTube videos into their apps or websites.

   Despite of this great opportunity that the technology presents the user, it also increases

the level of vulnerability to their data. Cyber-criminals have more opportunities to take advantage of thanks to these vulnerabilities

9. **Loss of data**
   Data stored on cloud servers can be lost through a natural disaster, malicious attacks, or a data wipe by the service provider. Losing sensitive data is devastating to firms, especially if they have no recovery plan. Google is an example of the big tech firms that have suffered permanent data loss after being struck by lightning four times in its power supply lines.

   Amazon was another firm that lost its essential customer data back in 2011.
   An essential step in securing data is carefully reviewing the terms of service of your provider and their back up procedures. The backup protocol could relate to physical access, storage locations, and natural disasters.

10. **Diminished customer trust**
    It is inevitable for customers to feel unsafe after data breach concerns at your firm. There have been massive security breaches that resulted in the theft of millions of customer credit and debit card numbers from data storage facilities.

    The breaches reduce customer trust in the security of their data. A breach in an organization's data will inevitably lead to a loss of customers, which ultimately impacts the firm's revenue.

11. **Increased customer agitation**
    A growing number of cloud service critics are keen to see which service providers have weak security protocols and encourage customers to avoid them. Most of these critics are popular around the internet and could lead to a poor impression of your firm in a few posts.
    If your customers suspect that their data is not safe in your hands, they not only move to competitor firms but also damage your firm's reputation.
12. **Revenue losses**
    Customers of a store will avoid buying from the store in the wake of news of data breach in the organization. A well known company as Target estimated a data breach in its platform to cost around $128 million. The CEO of the company resigned, and the company's directors remain under oversight by cyber security companies.

Software as a Service Security

SaaS providers handle much of the security for a cloud application. The SaaS provider is responsible for securing the platform, network, applications, operating system, and physical infrastructure. However, providers are not responsible for securing customer data or user access to it. Some providers offer a bare minimum of security, while others offer a wide range of SaaS security options.

The seven security issues which one should discuss with a cloud-computing vendor:

1. Privileged user access —inquire about who has specialized access to data, and about the hiring and management of such administrators.
2. Regulatory compliance—make sure that the vendor is willing to undergo external audits and/or security certifications.
3. Data location—does the provider allow for any control over the location of data?

4. Data segregation —make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals.
5. Recovery —Find out what will happen to data in the case of a disaster. Do they offer complete restoration? If so, how long would that take?
6. Investigative support —Does the vendor have the ability to investigate any inappropriate or illegal activity?
7. Long-term viability —What will happen to data if the company goes out of business? How will data be returned, and in what format?

To address the security issues listed above, SaaS providers will need to incorporate and enhance security practices used by the managed service providers and develop new ones as the cloud computing environment evolves. The baseline security practices for the SaaS environment as currently formulated are discussed in the following sections.

- **Security Management (People)**: One of the most important actions for a security team is to develop a formal charter for the security organization and program. This will foster a shared vision among the team of what security leadership is driving toward and expects, and will also foster "ownership" in the success of the collective team. The charter should be aligned with the strategic plan of the organization or company the security team works for. Lack of clearly defined roles and responsibilities, and agreement on expectations, can result in a general feeling of loss and confusion among the security team about what is expected of them, how their skills and experienced can be leveraged, and meeting their performance goals. Morale among the team and pride in the team is lowered, and security suffers as a result.
- **Security Governance**: A security steering committee should be developed whose objective is to focus on providing guidance about security initiatives and alignment with business and IT strategies. A charter for the security team is typically one of the first deliverables from the steering committee. This charter must clearly define the roles and responsibilities of the security team and other groups involved in performing information security functions. Lack of a formalized strategy can lead to an unsustainable operating model and security level as it evolves. In addition, lack of attention to security governance can result in key needs of the business not being met, including but not limited to, risk management, security monitoring, application security, and sales support. Lack of proper governance and management of duties can also result in potential security risks being left unaddressed and opportunities to improve the business being missed because the security team is not focused on the key security functions and activities that are critical to the business.
- **Risk Management**: Effective risk management entails identification of technology assets; identification of data and its links to business processes, applications, and data stores; and assignment of ownership and custodial responsibilities. Actions should also include maintaining a repository of information assets. Owners have authority and accountability for information assets including protection requirements, and custodians implement confidentiality, integrity, availability, and privacy controls. A formal risk assessment process should be created that allocates security resources linked to business continuity.
- **Risk Assessment**: Security risk assessment is critical to helping the information security organization make informed decisions when balancing the dueling priorities of business utility and protection of assets. Lack of attention to completing formalized risk assessments can contribute to an increase in information security audit findings, can jeopardize certification goals, and can lead to inefficient and ineffective selection of

security controls that may not adequately mitigate information security risks to an acceptable level. A formal information security risk management process should proactively assess information security risks as well as plan and manage them on a periodic or as-needed basis. More detailed and technical security risk assessments in the form of threat modeling should also be applied to applications and infrastructure. Doing so can help the product management and engineering groups to be more proactive in designing and testing the security of applications and systems and to collaborate more closely with the internal security team. Threat modeling requires both IT and business process knowledge, as well as technical knowledge of how the applications or systems under review work.

- **Security Monitoring and Incident Response**: Centralized security information management systems should be used to provide notification of security vulnerabilities and to monitor systems continuously through automated technologies to identify potential issues. They should be integrated with network and other systems monitoring processes (e.g., security information management, security event management, security information and event management, and security operations centers that use these systems for dedicated 24/7/365 monitoring). Management of periodic, independent third-party security testing should also be included. Many of the security threats and issues in SaaS center around application and data layers, so the types and sophistication of threats and attacks for a SaaS organization require a different approach to security monitoring than traditional infrastructure and perimeter monitoring. The organization may thus need to expand its security monitoring capabilities to include application- and data-level activities. This may also require subject-matter experts in applications security and the unique aspects of maintaining privacy in the cloud. Without this capability and expertise, a company may be unable to detect and prevent security threats and attacks to its customer data and service stability.
- **Third-Party Risk Management**: As SaaS moves into cloud computing for the storage and processing of customer data, there is a higher expectation that the SaaS will effectively manage the security risks with third parties. Lack of a third-party risk management program may result in damage to the provider's reputation, revenue losses, and legal actions should the provider be found not to have performed due diligence on its third-party vendors.

Cloud Security Monitoring

Monitoring is a critical component of cloud security and management. Typically relying on automated solutions, cloud security monitoring supervises virtual and physical servers to continuously assess and measure data, application, or infrastructure behaviors for potential security threats. This assures that the cloud infrastructure and platform function optimally while minimizing the risk of costly data breaches.

Benefits of cloud security monitoring

Cloud monitoring provides an easier way to identify patterns and pinpoint potential security vulnerabilities in cloud infrastructure. As there's a general perception of a loss of control when valuable data is stored in the cloud, effective cloud monitoring can put companies more at ease with making use of the cloud for transferring and storing data.

When customer data is stored in the cloud, cloud monitoring can prevent loss of business and frustrations for customers by ensuring that their personal data is safe. The use of web services

can increase security risks, yet cloud computing offers many benefits for businesses, from accessibility to a better customer experience. Cloud monitoring is one initiative that enables companies to find the balance between the ability to mitigate risks and taking advantage of the benefits of the cloud – and it should do so without hindering business processes.

key best practices for Effective Monitoring of Cloud Security

1. **Stringent Data Control**

   One of the most efficacious measures for mitigating cloud security risks is gaining complete control over data across all endpoints. Using solutions that scan, assess and take action on the data, before its transition from an enterprise network, enables a robust defense against any data loss through the cloud. This further helps in avoiding vulnerabilities, such as uploading of sensitive files to unprotected cloud repositories.

2. **Securing the Code**

   Securing codes must be one of the top priorities, to eliminate risks from potential cyberthreats. During the development of codes for websites, the focus lies in selecting the right security development lifecycle (SDL), which aligns well with the delivery strategies of companies. Key benefits associated with secure SDL include continuous security, early risk detection, improved stakeholder awareness, and reduction of business risks.

3. **Separating Crucial Metrics**

   A software developer aims at learning features of cloud security monitoring while designing new software with specific security aspects. For the implementation of a monitoring strategy, key considerations must be emphasized such as

   a. Determination of the resource inventory utilized in the organization
   b. Mapping all attributes of data that the organization aims to gather
   c. Mutual decision appertaining to software that best suits the organization

   While several cloud security monitoring solutions have been launched, the above guidelines would help in the successful execution of online monitoring system practices.

4. **Patch Management**

   Unpatched software and system result in significant issues. Keeping an organization's environment secure by updating the systems regularly has become imperative. Key requirements for an organization to eliminate risks for their systems include asset inventory, vulnerability data gathered, and configuration for understanding the criticality of the risks associated. Organizations must consider preparing the checklist of important procedures and make sure to keep all updates in check for arresting the vulnerabilities before implementation into the live environment. An apt blend of vulnerability scanning and automatic patching allude lower impact of threats.

5. Automation

Scripting remains an essential feature in the cloud security monitoring, as monitoring and reporting processes can be scripted for enabling automation of systems. Organizations must focus on the implementation of the monitoring software owing to the virtual nature of operations on the cloud, even as automating the red-flag and logging system for real-time alerts.

6. Identity and Access Management

Identity and access management provides capabilities of provisioning and access control for users. Administrators can use the IAM to manage users and groups and implement granular permission rules to limit access to resources and APIs.

Organizations must ensure the policies created are attached to roles or groups instead of individual users to deprive unnecessary or excessive privileges or permissions to users. To stem any unauthorized access to resources, organizations must provision access to these resources using roles instead of giving separate set of credentials for access.

It must be made sure that users are provided minimal access privileges to resources, which would not restrict them to fulfil their responsibilities. All users must have a multifactor authentication for their individual accounts as a defensive strategy against any compromised account.

Organizations must also limit the number of users with administrative privileges. The access keys must be rotated on a regular basis, and standardized periodically for password expiration, ensuring inaccessibility to data with a potential stolen or lost key.

A strong password policy must be enforced, requiring a minimum of fourteen characters that contain at least one symbol, one uppercase letter and one number. Also, a password reset policy must be enforced to prevent users from using the password used in the past 24 resets.

7. Data Protection

New technologies entail distinct issues and with the cloud-based storage solutions on the fore, data protection has become an imperative challenge to be addressed.

Organizations must opt for the cloud service providers that deliver data encryption as a standard feature in their offerings. Encrypting highly sensitive data including personally identifiable information (PII) or protected health information with the aid of customer-controlled keys has become a must-have for organizations eyeing the move to cloud. Customer-controlled key put the pressure of management on the customer, however they provide better control.

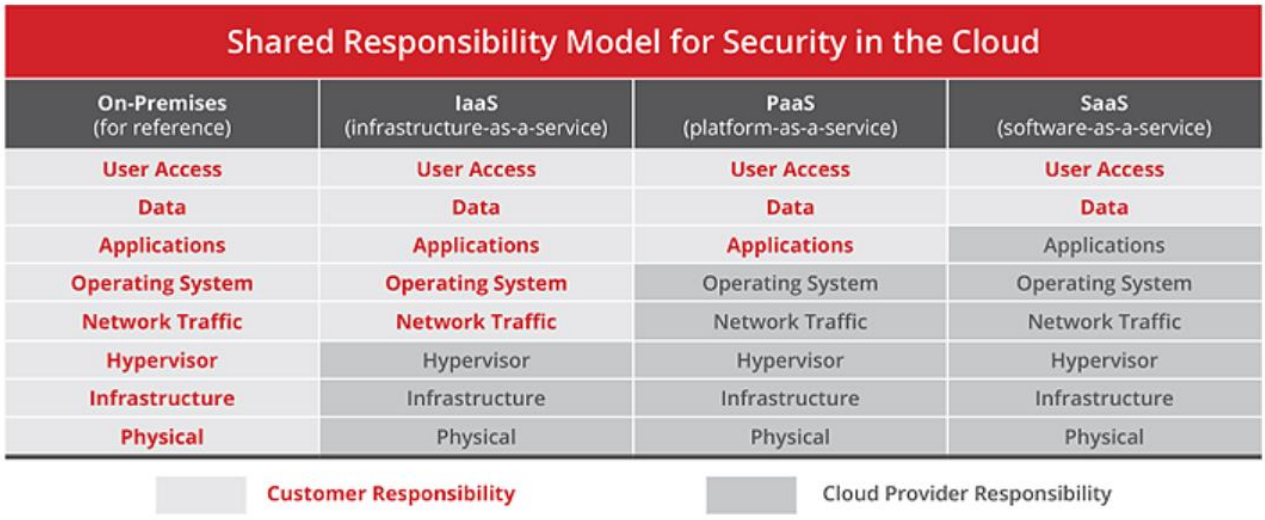
Organizations must choose the provider who guarantees protection against loss of critical data and meet the needs of data backup and recovery. Data replication is a common practice among the cloud service providers to ensure persistence. Organizations must thoroughly analyze the cloud deployment to identify where the replicated data has been cached or stored and take actions accordingly to ensure that the copied data has been deleted.

Security Architecture Design

When we need to explain cloud computing security architecture, it is important to get a clear idea about cloud computing and what are the safety measures it has been taking to protect the data. In general, we use cloud service providers (CSP) and service level agreements (SLA) to provide basic security to the stored data. Apart from these, several researchers also recommended some safety measures for cloud security architecture to protect the data at a basic level. They are-

- To monitor the cloud data easily. It is advisable to use a single sign-in ID for multiple accounts.
- Always prefer virtual firewalls and virtual comments to avoid threats.
- Maintain preventive measures for the Incorporated data.

The cloud security architecture plan may vary from model to model. So it is necessary to understand cloud computing security architecture for every model separately.



IaaS Cloud Computing Security Architecture

Infrastructure as a service architecture has majorly security and networking tools to protect the network of data. Hear the application programming interface impact is high rather than the other. Even though the cloud service provider's (CSP) provides security for the infrastructure, the remaining Security will be provided by Network tools like network packet brokers (NPB). The attributes of IaaS Cloud Computing Security Architecture are,

- Segmentation of the network will be in practice.
- Virtual Network tools are stored in the cloud.
- Virtual firewalls and web applications were preferred to use. It helps to prevent malware or threats.
- Optimum utilization of Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS).
- Virtual routers are also introduced.

SaaS Cloud Computing Security Architecture

The cloud security architecture in cloud computing follows a different plan for software as a service. as the name itself specifies that the Cloud security architecture majorly monitors the software and the data can be accessed with the help of the Internet's connection for the management. Management needs to negotiate with the CSP team to maintain proper security based on the legal contract between the security team and the management. Cloud access security brokers play a vital role in this Security model. The features of SaaS Cloud Computing Security Architecture are,

- Usage of multiple logs is highly prioritized.
- IP restrictions were strictly followed to maintain the security concerning management also.
- Application programming interface gateways are also used In This Cloud computing security architecture plan.

PaaS Cloud Computing Security Architecture

In general, the platform as a service model can be defined as the deployment of applications that can be done by considering the capabilities of the host and underlying software and hardware. But it doesn't consider the cost and complexity of buying those applications. Cloud security reference architecture for Paas majorly depends on the cloud security providers. As we already know that the applications can be taken care of by the management, the remaining data needs to look after by CSPs. Features of PaaS Cloud Computing Security Architecture are mostly similar to that of the SaaS plan. They are-

- Maintenance of several logs and audits.
- Do not get compromised with IP restrictions.
- Half of the security can be achieved by API gateways
- CASB Cloud access security brokers also had a significant part in maintaining security.

Application Security

Application security describes security measures at the application level that aim to prevent data or code within the app from being stolen or hijacked. It encompasses the security considerations that happen during application development and design, but it also involves systems and approaches to protect apps after they get deployed.

Application security may include hardware, software, and procedures that identify or minimize security vulnerabilities. A router that prevents anyone from viewing a computer's IP address from the Internet is a form of hardware application security. But security measures at the application level are also typically built into the software, such as an application firewall that strictly defines what activities are allowed and prohibited. Procedures can entail things like an application security routine that includes protocols such as regular testing.

Types of application security

Different types of application security features include authentication, authorization, encryption, logging, and application security testing. Developers can also code applications to reduce security vulnerabilities.

- **Authentication**: When software developers build procedures into an application to ensure that only authorized users gain access to it. Authentication procedures ensure that a user is who they say they are. This can be accomplished by requiring the user to provide a user name and password when logging in to an application. Multi-factor authentication requires more than one form of authentication—the factors might include something you know (a password), something you have (a mobile device), and something you are (a thumb print or facial recognition).
- **Authorization**: After a user has been authenticated, the user may be authorized to access and use the application. The system can validate that a user has permission to access the application by comparing the user's identity with a list of authorized users. Authentication must happen before authorization so that the application matches only validated user credentials to the authorized user list.
- **Encryption**: After a user has been authenticated and is using the application, other security measures can protect sensitive data from being seen or even used by a cybercriminal. In cloud-based applications, where traffic containing sensitive data travels between the end user and the cloud, that traffic can be encrypted to keep the data safe.
- **Logging**: If there is a security breach in an application, logging can help identify who got access to the data and how. Application log files provide a time-stamped record of which aspects of the application were accessed and by whom.
- **Application security testing**: A necessary process to ensure that all of these security controls work properly.

What are application security controls?

Application security controls are techniques to enhance the security of an application at the coding level, making it less vulnerable to threats. Many of these controls deal with how the application responds to unexpected inputs that a cybercriminal might use to exploit a weakness. A programmer can write code for an application in such a way that the programmer has more control over the outcome of these unexpected inputs. Fuzzing is a type of application security

testing where developers test the results of unexpected values or inputs to discover which ones cause the application to act in an unexpected way that might open a security hole.

Virtual Machine Security

Security is a problem. Network security is an even bigger problem because of the complex factors that define risks and the profound negative effects that can occur if you fail.

Virtual network security is the worst problem of all because it combines issues generated by traditional hosting and application security with those from network security, and then adds the challenges of virtual resources and services. It's no wonder we're only now starting to recognize the problems of cloud-virtual networking. And we're a long way from solving them.

Security should always be viewed as an incremental matter. How much different is the current situation than situations already experienced, tolerated or addressed? In the case of cloud-virtual security for networks, the biggest difference is virtual-to-resource mapping, meaning the framework required to connect hosted components. In short, cloud-virtual service security issues occur because security tools designed to protect hosted software features are different than those safeguarding physical devices.

Protect hosted elements by segregating them

Step one in securing virtual machine security in cloud computing is to *isolate the new hosted elements*. For example, let's say three features hosted inside an edge device could be deployed in the cloud either as part of the service data plane, with addresses visible to network users, or as part of a private subnetwork that's invisible. If you deploy in the cloud, then any of the features can be attacked, and it's also possible your hosting and management processes will become visible and vulnerable. If you isolate your hosting and feature connections inside a private subnetwork, they're protected from outside access.

In container hosting today, both in the data center and in the cloud, application components deploy inside a private subnetwork. As a result, only the addresses representing APIs that users are supposed to access are exposed. That same principle needs to be applied to virtual functions; expose the interfaces that users actually connect to and hide the rest with protected addresses.

Ensure all components are tested and reviewed

Step two in cloud-virtual security is to *certify virtual features and functions for security compliance before you allow them to be deployed*. Outside attacks are a real risk in virtual networking, but an insider attack is a disaster. If a feature with a back-door security fault is introduced into a service, it becomes part of the service infrastructure and is far more likely to possess open attack vectors to other infrastructure elements.

Private subnetworks can help in addressing virtual machine security in cloud computing. If new components can only access other components in the same service instance, the risk is reduced that malware can be introduced in a new software-hosted feature. Yes, a back-door attack could put the service itself at risk, but it's less likely the malware will spread to other services and customers.

This approach, however, doesn't relieve operators of the burden of security testing. It's important to insist on a strong lifecycle management compliance process flow for all hosted features and functions -- one that operators can audit and validate. If the companies supplying your hosted features or functions properly test their new code, it's less likely it will contain accidental vulnerabilities or deliberately introduced back-door faults.

Separate management APIs to protect the network

Step three is to *separate infrastructure management and orchestration from the service*. Management APIs will always represent a major risk because they're designed to control features, functions and service behavior. It's important to protect all such APIs, but it's critical to protect the APIs that oversee infrastructure elements that should never be accessed by service users.

The most important area to examine to ensure virtual machine security in cloud computing is the virtual-function-specific piece of the Virtual Network Functions Manager (VNFM) structure mandated by the ETSI NFV (Network Functions Virtualization) Industry Specification Group. This code is provided by the suppler of the VNF, and it is likely to require access to APIs that represent infrastructure elements as well as orchestration or deployment tools. Nothing more than bad design is needed for these elements to open a gateway to infrastructure management APIs that could affect the security and stability of features used in virtual-cloud services.

Securing the VNFM means requiring that providers of VNFs offer their architectures governing VNFM connections to infrastructure or deployment/management APIs for review and possible security enhancements. The important point is to ensure that no service user, VNF or VNFM associated with other VNFs or services can access an infrastructure management API.

By containing access, you limit your security risk. Additionally, operators should require that access to infrastructure management and orchestration APIs by any source is chronicled, and that any access or change is reviewed to prevent a management access leak from occurring.

Keep connections secure and separate

The fourth and final point in cloud-virtual network security is to *ensure that virtual network connections don't cross over between tenants or services*. Virtual networking is a wonderful way of creating agile connections to redeployed or scaled features, but each time a virtual network change is made, it's possible it can establish an inadvertent connection between two different services, tenants or feature/function deployments. This can produce a data plane leak, a connection between the actual user networks or a management or control leak that could allow one user to influence the service of another.

Ironclad practices and policies governing virtual connectivity can reduce the risk of an error like this, but it's very difficult to prevent one altogether. That's because of the indirect relationship between a virtual network that connects features and a real network that connects users. One remedy is to use a network scanner or inventory tool to search for devices and virtual devices on a virtual network and compare that result with the service topology that's expected. This can be run as the last step of a virtual network change.

Cloud-virtual networking introduces the cloud to networking, but it can also usher in server, hosting and virtual network security issues as well. Anyone who thinks these risks can be addressed through traditional means -- using tools and practices from the era when we built networks only from devices -- is going to face a hard reality, and soon.

Identity Management and Access Control

An Identity and Access Management (IAM) system defines and manages user identities and access permissions. Users of IAM include customers (customer identity management) and employees (employee identity management). With IAM technologies, IT managers can ensure

that users are who they say they are (authentication) and that users access the applications and resources they have permission to use (authorization).

4 Key Benefits of Identity and Access Management Systems

1. **Eliminating weak passwords**—research shows over 80% of data breaches are caused by stolen, default, or weak passwords. IAM systems enforce best practices in credential management, and can practically eliminate the risk that users will use weak or default passwords. They also ensure users frequently change passwords.
2. **Mitigating insider threats**—a growing number of breaches is caused by insiders. IAM can limit the damage caused by malicious insiders, by ensuring users only have access to the systems they work with, and cannot escalate privileges without supervision.
3. **Advanced tracking of anomalies**—modern IAM solutions go beyond simple credential management, and include technologies such as machine learning, artificial intelligence, and risk-based authentication, to identify and block anomalous activity.
4. **Multi-factor security**—IAM solutions help enterprises progress from two-factor to three-factor authentication, using capabilities like iris scanning, fingerprint sensors, and face recognition.

Why is IAM so important for cloud computing?

In cloud computing, data is stored remotely and accessed over the Internet. Because users can connect to the Internet from almost any location and any device, most cloud services are device- and location-agnostic. Users no longer need to be in the office or on a company-owned device to access the cloud. And in fact, remote workforces are becoming more common.

As a result, identity becomes the most important point of controlling access, not the network perimeter. The user's identity, not their device or location, determines what cloud data they can access and whether they can have any access at all.

To understand why identity is so important, here's an illustration. Suppose a cyber-criminal wants to access sensitive files in a company's corporate datacenter. In the days before cloud computing was widely adopted, the cyber-criminal would have to get past the corporate firewall protecting the internal network or physically access the server by breaking into the building or bribing an internal employee. The criminal's main goal would be to get past the network perimeter.

However, with cloud computing, sensitive files are stored in a remote cloud server. Because employees of the company need to access the files, they do so by logging in via browser or an

app. If a cyber-criminal wants to access the files, now all they need is employee login credentials (like a username and password) and an Internet connection; the criminal doesn't need to get past a network perimeter.