Cloud network security is a vital part of an organization's overall cybersecurity strategy. As more companies shift their operations to the cloud, it's critical for security analysts to understand how to protect data, applications, and resources in this environment. Here’s a breakdown of the key concepts from your video:

Cloud Networks and Their Importance

* A cloud network is a collection of remote servers or computers that provide storage, processing, and data analytics over the internet.
* Cloud networks allow companies to host data and applications, offering on-demand scalability and flexibility.
* Despite the advantages, cloud networks are still susceptible to intrusions by internal and external malicious actors.

Key Cloud Security Practices

1. Baseline Image for Cloud Servers
   * What it is: A server baseline image is a documented configuration of the server (similar to a traditional baseline) that defines its expected state.
   * Why it’s important: Baselines allow analysts to compare the current state of cloud servers with the baseline image. Any unauthorized changes can indicate an intrusion.
   * Best Practice: Use the baseline image for all server instances in the cloud to standardize and secure deployments.
2. Data and Application Segregation
   * What it is: Separating data and applications in the cloud based on their service category or function.
   * Examples:
     + Separate older applications from newer ones to avoid compatibility issues.
     + Isolate internal software from front-end, user-facing applications.
   * Why it’s important: Prevents issues in one area (e.g., a compromised front-end application) from impacting critical internal systems.
3. Shared Responsibility Model
   * What it is: Cloud security responsibilities are divided between the cloud service provider and the organization using their services.
   * Provider’s Role: Typically responsible for securing the physical infrastructure and the core cloud platform.
   * Organization’s Role: Responsible for securing data, applications, and configurations within the cloud environment.
   * Best Practice: Understand and comply with the shared responsibility model to avoid security gaps.

Cloud Network Hardening Techniques

Many of the techniques used in traditional network hardening also apply to cloud environments, with some adaptations:

1. Firewall Configuration
   * Apply cloud firewalls or security groups to control incoming and outgoing traffic for virtual machines or cloud resources.
   * Block unnecessary ports and restrict traffic to authorized IP addresses.
2. Encryption
   * Use end-to-end encryption to secure data in transit and encryption at rest for stored data.
   * Leverage the latest encryption standards, such as AES-256, to ensure data is secure.
3. Access Controls
   * Implement least privilege access for all cloud resources.
   * Use Identity and Access Management (IAM) tools provided by the cloud service provider to enforce strict access policies.
4. Monitoring and Logging
   * Enable cloud-native monitoring tools like AWS CloudTrail, Google Cloud Logging, or Azure Monitor to track user activity and detect unusual events.
   * Analyze cloud logs regularly to identify potential security incidents.
5. Regular Updates and Patch Management
   * Ensure all virtual machines, containers, and cloud-based applications are updated regularly with the latest patches.
6. Multi-Factor Authentication (MFA)
   * Require MFA for all access to cloud platforms and applications to provide an additional layer of security.
7. Network Segmentation
   * Use virtual private clouds (VPCs) or subnets to segment sensitive resources from public-facing applications.
   * Limit communication between these segments using security policies.

Why Cloud Security Matters

* Protects Sensitive Data: Cloud networks often host critical company data, and a breach can have devastating consequences.
* Maintains Business Continuity: A secure cloud network ensures that operations remain uninterrupted.
* Meets Compliance Standards: Many industries have specific regulations for cloud security, such as HIPAA for healthcare or GDPR for data privacy.

By following these practices and understanding the shared responsibility model, organizations can create a more secure cloud environment. Let me know if you'd like to explore any of these topics further!

# Secure the cloud

Earlier in this course, you were introduced to [cloud computing](https://www.coursera.org/learn/networks-and-network-security/lecture/BGlnq/cloud-networks)

. **Cloud computing** is a model for allowing convenient and on-demand network access to a shared pool of configurable computing resources. These resources can be configured and released with minimal management effort or interaction with the service provider.

Just like any other IT infrastructure, a cloud infrastructure needs to be secured. This reading will address some main security considerations that are unique to the cloud and introduce you to the shared responsibility model used for security in the cloud. Many organizations that use cloud resources and infrastructure express concerns about the privacy of their data and resources. This concern is addressed through cryptography and other additional security measures, which will be discussed later in this course.

## Cloud security considerations

Many organizations choose to use cloud services because of the ease of deployment, speed of deployment, cost savings, and scalability of these options. Cloud computing presents unique security challenges that cybersecurity analysts need to be aware of.

### Identity access management

**Identity access management (IAM)** is a collection of processes and technologies that helps organizations manage digital identities in their environment. This service also authorizes how users can use different cloud resources. A common problem that organizations face when using the cloud is the loose configuration of cloud user roles. An improperly configured user role increases risk by allowing unauthorized users to have access to critical cloud operations.

### Configuration

The expanding cloud ecosystem introduces significant complexity to network management. Each cloud service necessitates precise configuration to uphold security and compliance standards. This challenge intensifies during cloud migrations, where ensuring accurate configuration for every migrated process is critical. Neglect in this area can expose the network to vulnerabilities. Misconfigured cloud services are a frequent source of security breaches, underscoring the importance of meticulous attention to detail by network administrators and architects during the migration and ongoing management of cloud services.

### Attack surface

Cloud service providers (CSPs) offer numerous applications and services for organizations at a low cost.

Every service or application on a network carries its own set of risks and vulnerabilities and increases an organization’s overall attack surface. An increased attack surface must be compensated for with increased security measures.

Cloud networks that utilize many services introduce lots of entry points into an organization’s network. However, if the network is designed correctly, utilizing several services does not introduce more entry points into an organization’s network design. These entry points can be used to introduce malware onto the network and pose other security vulnerabilities. It is important to note that CSPs often defer to more secure options, and have undergone more scrutiny than a traditional on-premises network.

### Zero-day attacks

Zero-day attacks are an important security consideration for organizations using cloud or traditional on-premise network solutions. A **zero day** attack is an exploit that was previously unknown. CSPs are more likely to know about a zero day attack occurring before a traditional IT organization does. CSPs have ways of patching hypervisors and migrating workloads to other virtual machines. These methods ensure the customers are not impacted by the attack. There are also several tools available for patching at the operating system level that organizations can use.

### Visibility and tracking

Network administrators have access to every data packet crossing the network with both on-premise and cloud networks. They can sniff and inspect data packets to learn about network performance or to check for possible threats and attacks.

This kind of visibility is also offered in the cloud through flow logs and tools, such as packet mirroring. CSPs take responsibility for security in the cloud, but they do not allow the organizations that use their infrastructure to monitor traffic on the CSP’s servers. Many CSPs offer strong security measures to protect their infrastructure. Still, this situation might be a concern for organizations that are accustomed to having full access to their network and operations. CSPs pay for third-party audits to verify how secure a cloud network is and identify potential vulnerabilities. The audits can help organizations identify whether any vulnerabilities originate from on-premise infrastructure and if there are any compliance lapses from their CSP.

### Things change fast in the cloud

CSPs are large organizations that work hard to stay up-to-date with technology advancements. For organizations that are used to being in control of any adjustments made to their network, this can be a potential challenge to keep up with. Cloud service updates can affect security considerations for the organizations using them. For example, connection configurations might need to be changed based on the CSP’s updates.

Organizations that use CSPs usually have to update their IT processes. It is possible for organizations to continue following established best practices for changes, configurations, and other security considerations. However, an organization might have to adopt a different approach in a way that aligns with changes made by the CSP.

Cloud networking offers various options that might appear attractive to a small company—options that they could never afford to build on their own premises. However, it is important to consider that each service adds complexity to the security profile of the organization, and they will need security personnel to monitor all of the cloud services.

## Shared responsibility model

A commonly accepted cloud security principle is the shared responsibility model. The **shared responsibility model** states that the CSP must take responsibility for security involving the cloud infrastructure, including physical data centers, hypervisors, and host operating systems. The company using the cloud service is responsible for the assets and processes that they store or operate in the cloud.

The shared responsibility model ensures that both the CSP and the users agree about where their responsibility for security begins and ends. A problem occurs when organizations assume that the CSP is taking care of security that they have not taken responsibility for. One example of this is cloud applications and configurations. The CSP takes responsibility for securing the cloud, but it is the organization’s responsibility to ensure that services are configured properly according to the security requirements of their organization.

## Key takeaways

It is essential to know the security considerations that are unique to the cloud and understanding the shared responsibility model for cloud security. Organizations are responsible for correctly configuring and maintaining best security practices for their cloud services. The shared responsibility model ensures that both the CSP and users agree about what the organization is responsible for and what the CSP is responsible for when securing the cloud infrastructure.

# Cryptography and cloud security

Earlier in this course, you were introduced to the concepts of the shared responsibility model and identity and access management (IAM). Similar to on-premise networks, cloud networks also need to be secured through a mixture of security hardening practices and cryptography.

This reading will address common cloud security hardening practices, what to consider when implementing cloud security measures, and the fundamentals of cryptography. Since cloud infrastructure is becoming increasingly common, it’s important to understand how cloud networks operate and how to secure them.

## Cloud security hardening

There are various techniques and tools that can be used to secure cloud network infrastructure and resources. Some common cloud security hardening techniques include incorporating IAM, hypervisors, baselining, cryptography, and cryptographic erasure.

### Identity access management (IAM)

**Identity access management (IAM)** is a collection of processes and technologies that helps organizations manage digital identities in their environment. This service also authorizes how users can leverage different cloud resources.

### Hypervisors

A **hypervisor** abstracts the host’s hardware from the operating software environment. There are two types of hypervisors. Type one hypervisors run on the hardware of the host computer. An example of a type one hypervisor is VMware®'s ESXi. Type two hypervisors operate on the software of the host computer. An example of a type two hypervisor is VirtualBox. Cloud service providers (CSPs) commonly use type one hypervisors. CSPs are responsible for managing the hypervisor and other virtualization components. The CSP ensures that cloud resources and cloud environments are available, and it provides regular patches and updates. Vulnerabilities in hypervisors or misconfigurations can lead to virtual machine escapes (VM escapes). A VM escape is an exploit where a malicious actor gains access to the primary hypervisor, potentially the host computer and other VMs. As a CSP customer, you will rarely deal with hypervisors directly.

### Baselining

Baselining for cloud networks and operations cover how the cloud environment is configured and set up. A baseline is a fixed reference point. This reference point can be used to compare changes made to a cloud environment. Proper configuration and setup can greatly improve the security and performance of a cloud environment. Examples of establishing a baseline in a cloud environment include: restricting access to the admin portal of the cloud environment, enabling password management, enabling file encryption, and enabling threat detection services for SQL databases.

## Cryptography in the cloud

Cryptography can be applied to secure data that is processed and stored in a cloud environment. Cryptography uses encryption and secure key management systems to provide data integrity and confidentiality. Cryptographic encryption is one of the key ways to secure sensitive data and information in the cloud.

Encryption is the process of scrambling information into ciphertext, which is not readable to anyone without the encryption key. Encryption primarily originated from manually encoding messages and information using an algorithm to convert any given letter or number to a new value. Modern encryption relies on the secrecy of a key, rather than the secrecy of an algorithm. Cryptography is an important tool that helps secure cloud networks and data at rest to prevent unauthorized access. You’ll learn more about cryptography in-depth in an upcoming course.

## Cryptographic erasure

Cryptographic erasure is a method of erasing the encryption key for the encrypted data. When destroying data in the cloud, more traditional methods of data destruction are not as effective. Crypto-shredding is a newer technique where the cryptographic keys used for decrypting the data are destroyed. This makes the data undecipherable and prevents anyone from decrypting the data. When crypto-shredding, all copies of the key need to be destroyed so no one has any opportunity to access the data in the future.

## Key Management

Modern encryption relies on keeping the encryption keys secure. Below are the measures you can take to further protect your data when using cloud applications:

* Trusted platform module (TPM). TPM is a computer chip that can securely store passwords, certificates, and encryption keys.
* Cloud hardware security module (CloudHSM). CloudHSM is a computing device that provides secure storage for cryptographic keys and processes cryptographic operations, such as encryption and decryption.

Organizations and customers do not have access to the cloud service provider (CSP) directly, but they can request audits and security reports by contacting the CSP. Customers typically do not have access to the specific encryption keys that CSPs use to encrypt the customers’ data. However, almost all CSPs allow customers to provide their own encryption keys, depending on the service the customer is accessing. In turn, the customer is responsible for their encryption keys and ensuring the keys remain confidential. The CSP is limited in how they can help the customer if the customer’s keys are compromised or destroyed. One key benefit of the shared responsibility model is that the customer is not entirely responsible for maintenance of the cryptographic infrastructure. Organizations can assess and monitor the risk involved with allowing the CSP to manage the infrastructure by reviewing a CSPs audit and security controls. For federal contractors, FEDRAMP provides a list of verified CSPs.

## Key takeaways

Cloud security hardening is a critical component to consider when assessing the security of various public cloud environments and improving the security within your organization. Identity access management (IAM), correctly configuring a baseline for the cloud environment, securing hypervisors, cryptography, and cryptographic erasure are all methods to use to further secure cloud infrastructure.