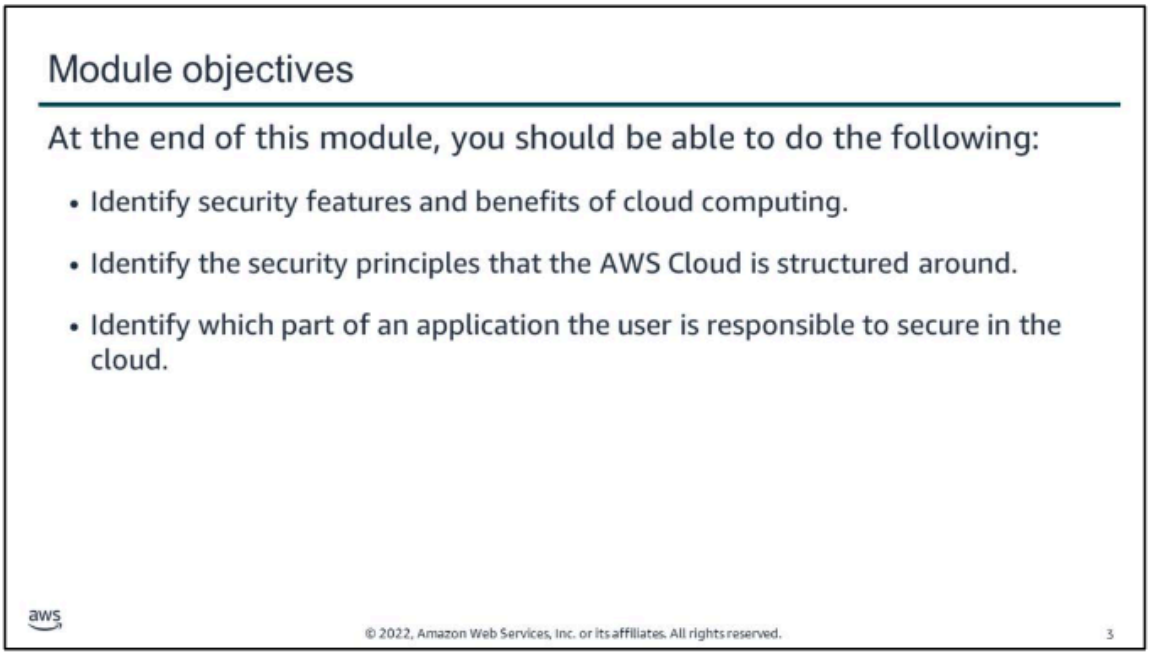
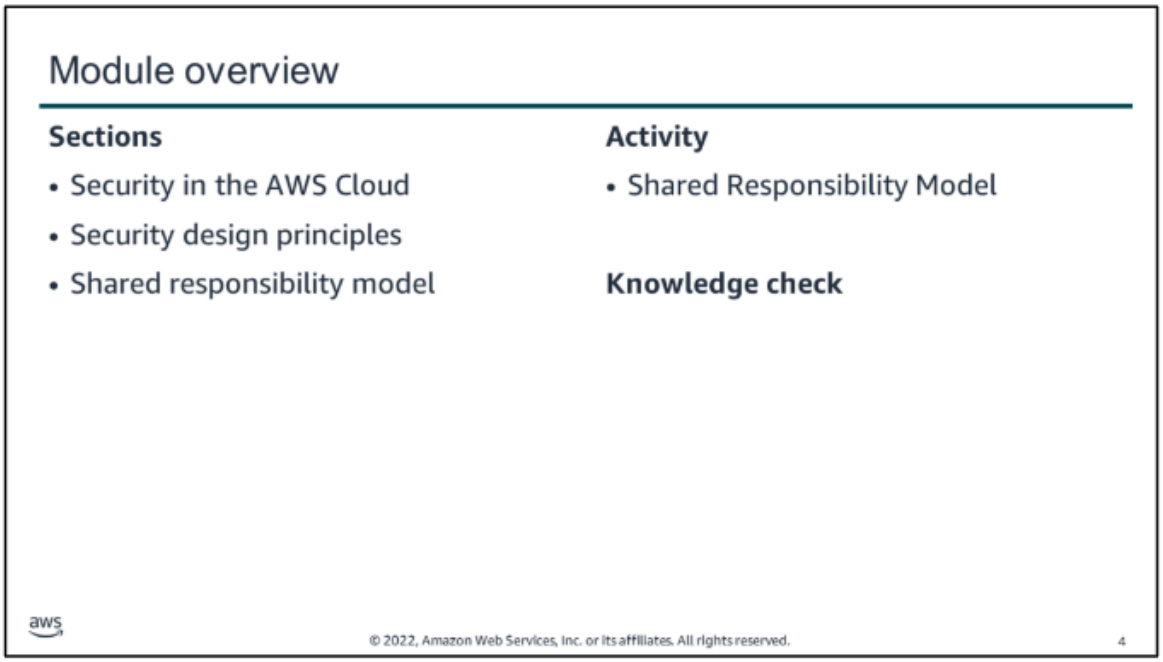
2 - Introduction To AWS Security

- Module Objectives



- Module Overview

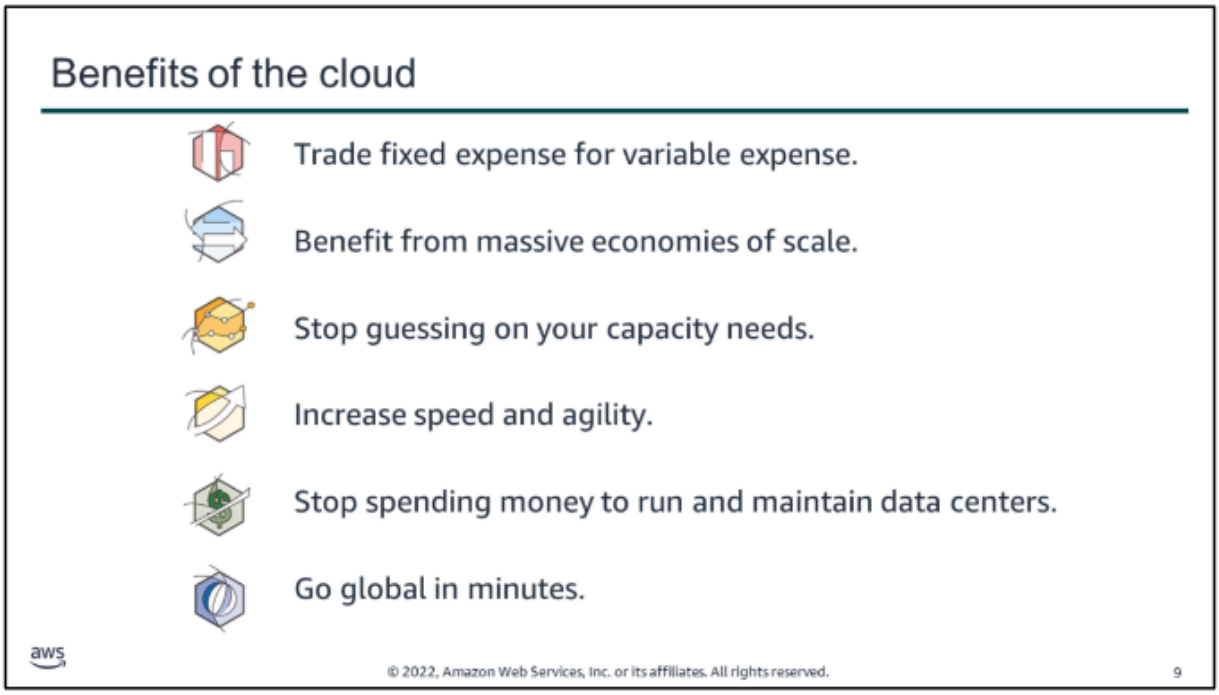


- Here, we'll try to learn and discover "The foundations of cloud security and the AWS shared responsibility model."
- Reminder : AWS are responsible of the security of the cloud, meanwhile The client is responsible of the security in the cloud...

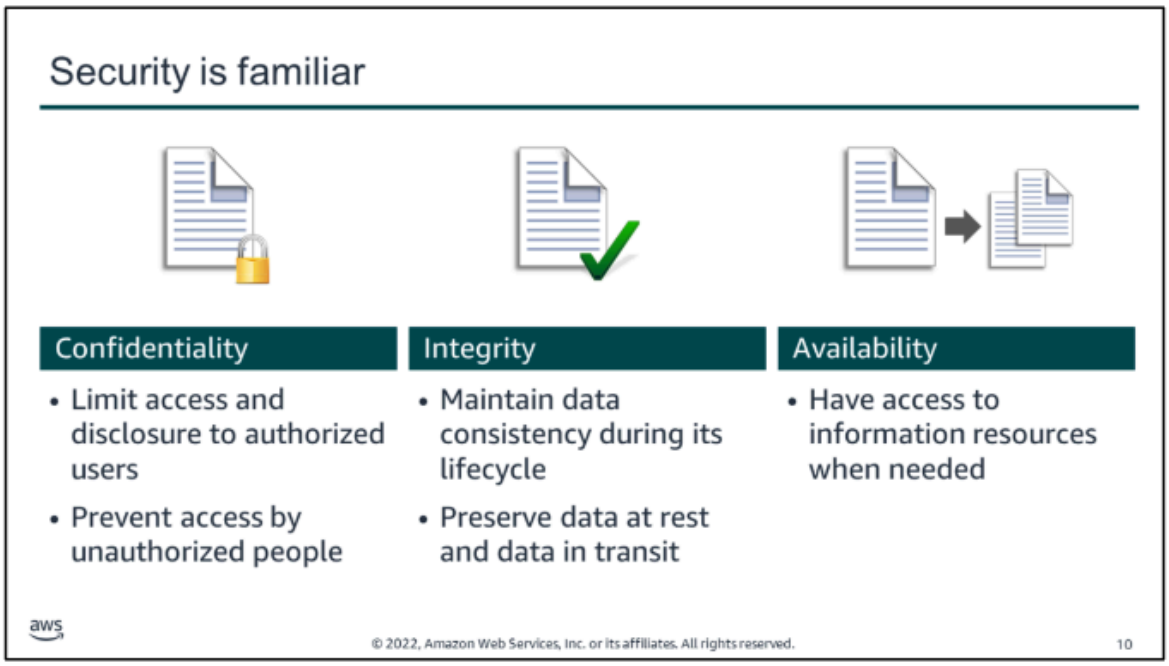
- So basically, there are parts of security in which the client is responsible of, and the other remaining parts concern AWS...

Security in AWS Cloud

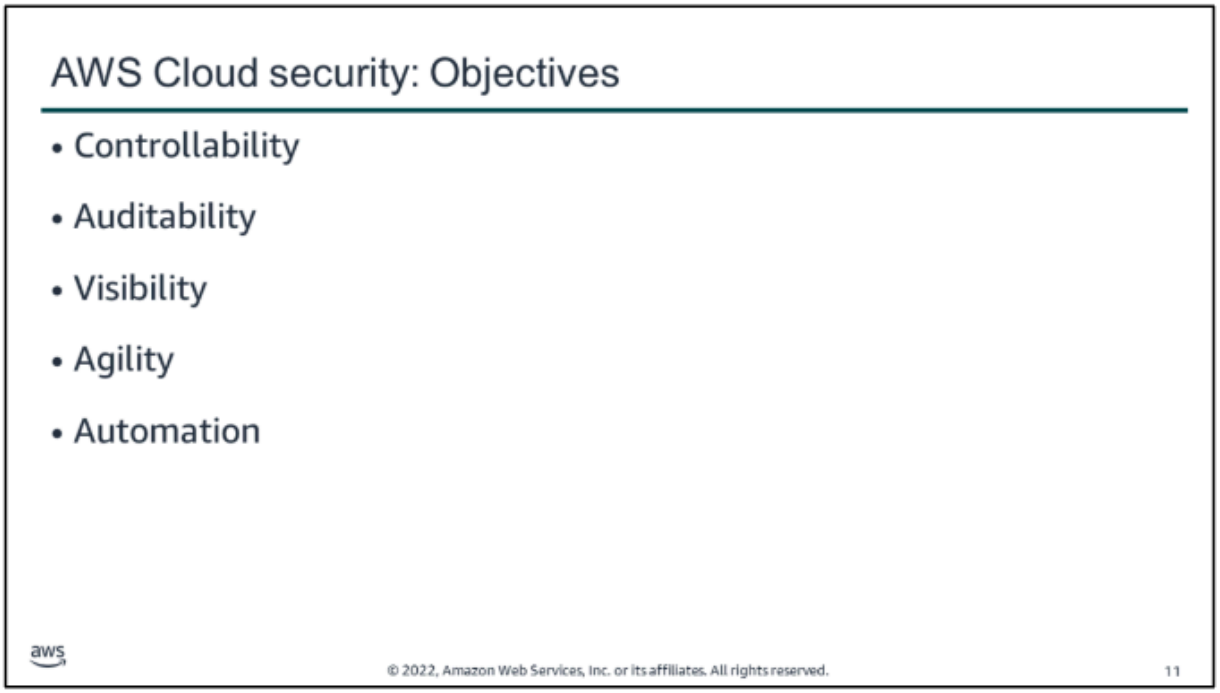
- A little reminder of the AWS Cloud benefits:



- Of course in AWS, security is based on the main & usual

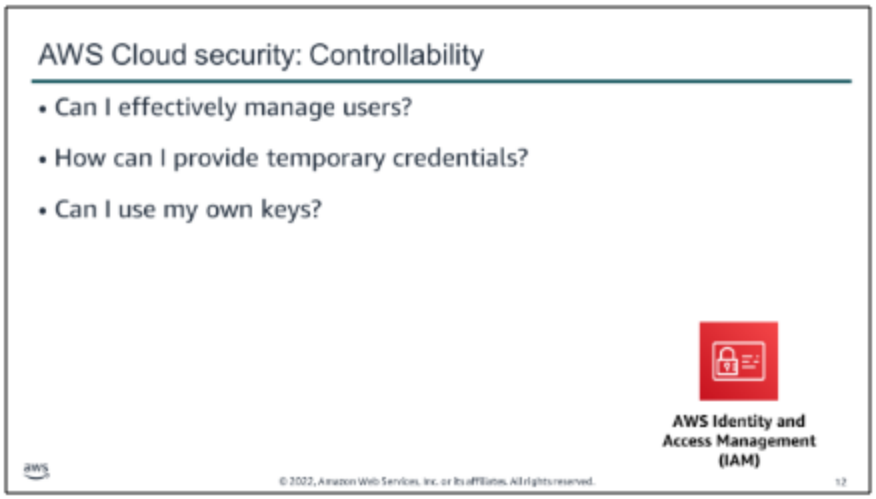


- Here are some detailed objectives of the security:



We start off with "Controllability":

- By Controllability, we mean :



- And here, our minds switch directly to services such as AWS IAM (Identity & Access Management) for user access to ressources control...
- For the temporary credentials (We give access to people temporarily with credentials to our ressources), we think immediately of AWS STS (Security Token Service)...
- For Keys security (such as encryption), we use AWS CloudHSM...

AWS provides methods and tools to manage access control for users, groups, and roles; provide temporary security credentials; and control encryption keys.

The AWS Identity and Access Management (IAM) service helps you securely control access to AWS resources for your users. Use IAM to control who can use your AWS resources (authentication), what resources they can use, and in what ways (authorization). You can define granular permissions for entities such as users, groups, or roles. This enables entities to administer and use resources in your AWS account without having to share your password or access key.

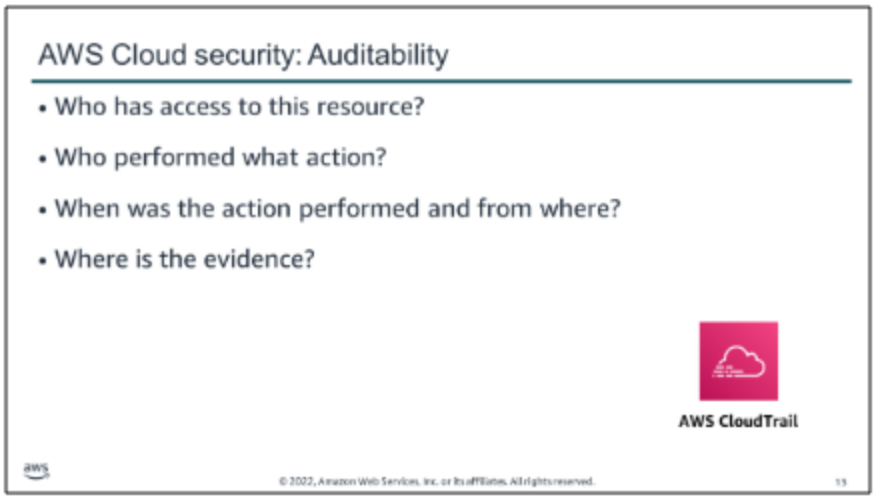
You can grant different permissions to different people for different resources. For example, you might allow some users complete access to Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), and other AWS services. For other users, you can allow read-only access to just some S3 buckets, permission to administer just some EC2 instances, or access to your billing information but nothing else. With IAM, you can also allow users who already have passwords elsewhere to access your AWS account. For example, users with passwords in your corporate network or with an internet identity provider can get access to your AWS account.

You can use the AWS Security Token Service (AWS STS) to create and provide trusted users with temporary security credentials that can control access to your AWS resources. Temporary security credentials work almost identically to the long-term access key credentials that your IAM users can use.

With AWS CloudHSM, you can protect your encryption keys within hardware security modules (HSMs) that are designed and validated to government standards for secure key management. You can securely generate, store, and manage the cryptographic keys used for data encryption in a way that ensures that only you have access to the keys. CloudHSM helps you comply with strict key management requirements within the AWS Cloud without sacrificing application performance.

Then we have "Auditability" :

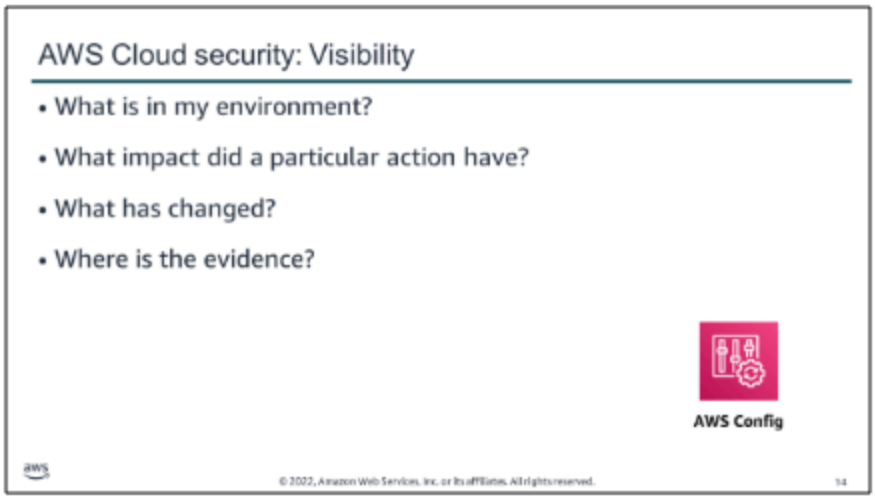
- Here, we talk about evidence, tracking, logs...



- Here we use AWS CloudTrail, which records activity and everything happening...

"Visibility" :

- Here we talk about our ressources, and our reliance on them and monitoring them and stuff...



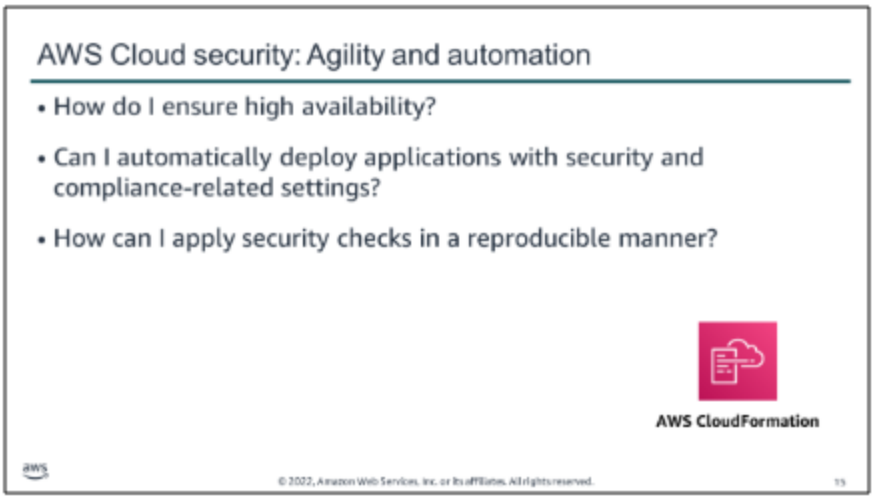
The first step to secure your assets is to know what they are. You shouldn't need to guess what your IT inventory consists of, who is accessing your resources, and what actions anyone has run on your resources.

AWS offers tools to keep track of and monitor your AWS resources, so you have instant visibility into your inventory, and your user and application activity. For example, by using AWS Config, you can discover existing AWS resources, export a complete inventory of your AWS resources with all configuration details, and determine how a resource was configured at any point in time. These capabilities can help you with compliance auditing, security analysis, resource change tracking, and troubleshooting.

- We can use AWS Config to manage ressources...

"Agility and Automation" :

- Here, we mainly talk about High Availability...

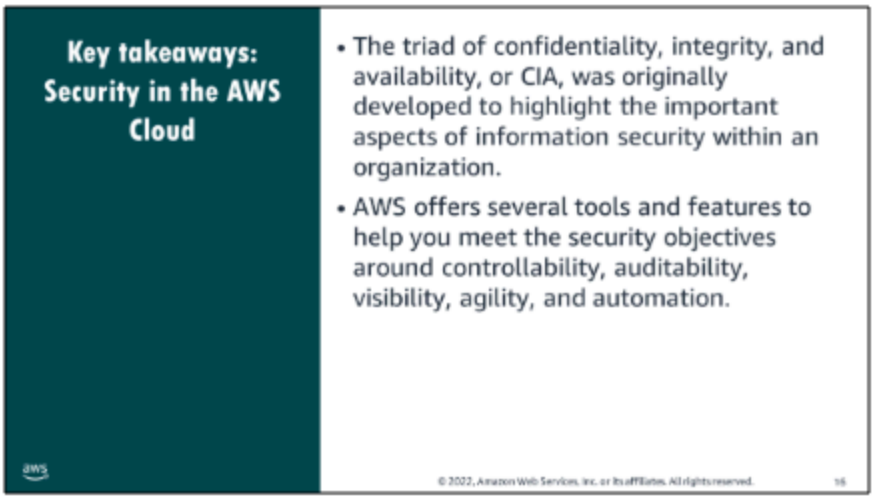


The increase in agility and the ability to perform actions faster, at a larger scale and at a lower cost, does not invalidate well-established principles of information security. Automatically scaling to ensure high availability during a security attack is one of the ways that AWS provides agility to meet needs. AWS designs data centers with excess bandwidth, so that if a major disruption occurs, sufficient capacity is available to load balance traffic and route it to remaining sites, to minimize the impact on our customers. Customers also use this multiple Region, multiple Availability Zone strategy to build highly resilient applications at a disruptively low cost, to easily replicate and back up data, and to deploy global security controls consistently across their business.

AWS tools are purpose built, and tailored to your unique environment, size, and global requirements. By building security tools from the ground up, AWS can automate many of the routine tasks that security experts normally spend time on. This means AWS security experts can spend more time focusing on measures to increase the security of your AWS Cloud environment. Customers can also automate security engineering and operations functions by using a comprehensive set of APIs and tools.

When you automate by using AWS services such as AWS CloudFormation, rather than manually deploying an environment for forensics troubleshooting, for example, you can have AWS deploy an environment in a secure and reproducible manner.

- Here, we can bring up EC2 Auto-Scaling and AWS CloudWatch

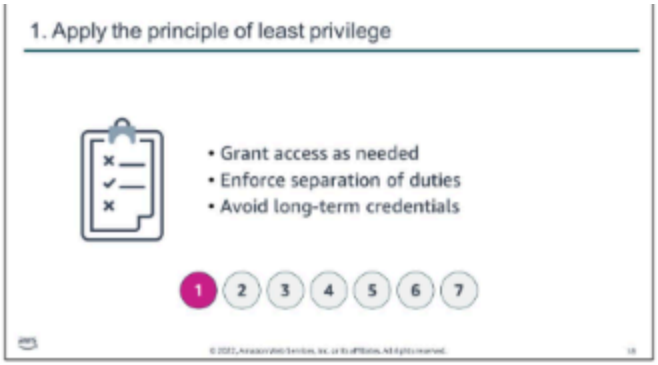


Key takeaways from this section of the module include the following:

- The triad of confidentiality, integrity, and availability, or CIA, was originally developed to highlight the important aspects of information security within an organization.
- AWS offers several tools and features to help you meet the security objectives around controllability, auditability, visibility, agility, and automation.

Security Design Principles

Apply the principle of least privilege :



This section describes the seven design principles from the security pillar of the AWS Well-Architected Framework. Following these principles can help you strengthen your workload security, and can help guide your conversations around security and compliance.

An organizational security culture should be built on the principle of least privilege. Only grant access to data and other resources to the people who really need that access. You can start with denying access to everything and grant access as needed, based on job role.

A security best practice is to enforce separation of duties with appropriate authorization for each interaction with your AWS resources. Set expectations for how authority will be delegated down through software engineers, operations staff, and other job functions that are involved in cloud adoption.

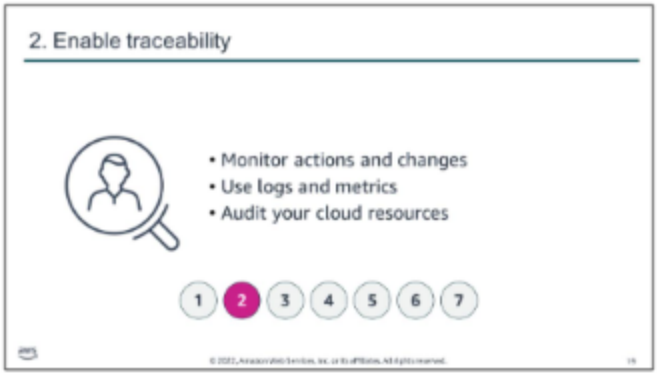
By reducing or even ending reliance on long-term credentials, you can diminish your attack surface area. You can use temporary credentials and require identities to dynamically acquire them. For workforce identities, use AWS Single Sign-On or federation with IAM to access AWS accounts. For machine identities, such as EC2 instances or AWS Lambda functions, require the use of IAM roles, instead of IAM users with long-term access keys.

Identity and access management are key parts of an information security program to ensure that only authorized and authenticated users and components are able to access your resources, and only in a manner that you intend. In AWS, IAM is the primary service for permissions management. The service provides the ability to control user and programmatic access to AWS services and resources.

With IAM, you can define principals (that is, accounts, users, roles, and services that can perform actions in your account) and build out granular policies aligned with these principals. You also have the ability to require strong password practices, such as setting a complexity level, avoiding re-use, and enforcing multi-factor authentication (MFA). You can use federation with your existing directory service. For workloads that require systems to have access to AWS, IAM can provide secure access through roles, instance profiles, identity federation, and temporary credentials.

- Here, there are some good tips for good security in AWS IAM for example...
- Like, denying access to everyone then giving access to people instead of the opposite...

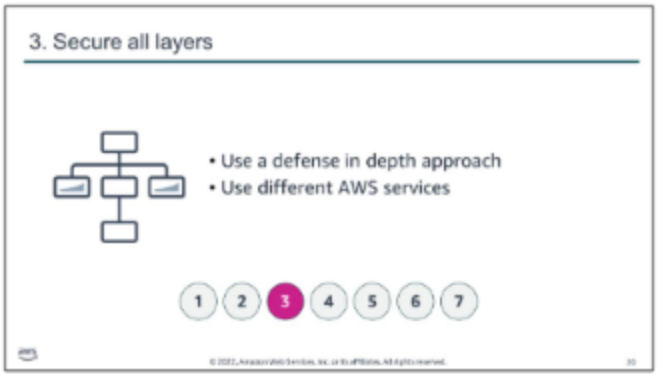
Enable Tracebility :



With AWS, you can monitor, alert, and audit actions and changes to your environment in real time. AWS provides native logging as well as services that you can use to provide greater visibility in near-real time for occurrences in your environment. Integrate these tools with your existing logging and monitoring solutions. Know what workloads are deployed and operational, so that you can audit and ensure that the environment is operating at expected security governance levels and meeting required security standards.

In AWS, you can implement detective controls by processing logs and events, and monitoring, which allows for auditing, automated analysis, and alarming. CloudTrail logs, AWS API calls, and Amazon CloudWatch provide monitoring of metrics with alarming, and AWS Config provides configuration history. Amazon GuardDuty is a managed threat detection service that continuously monitors for malicious or unauthorized behavior to help you protect your AWS accounts and workloads. Service-level logs are also available; for example, you can use Amazon S3 to log access requests.

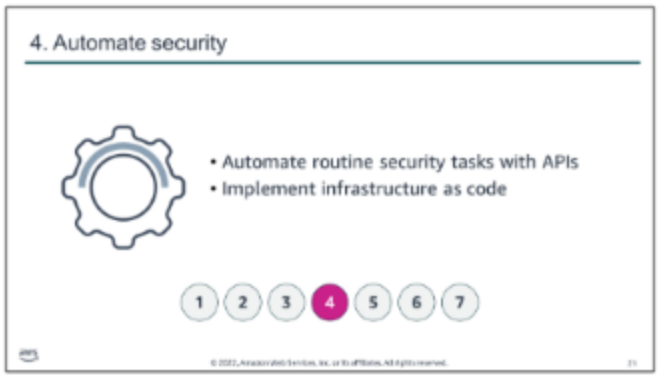
Secure All Layers :



Rather than only focusing on the protection of a single outer layer, apply a defense in depth approach with other security controls. This means to apply security to all layers, such as your network, application, and data store. For example, you can require users to strongly authenticate to an application. In addition, ensure that users come from a trusted network path and require access to the decryption keys to process encrypted data. One of the benefits of using AWS is that our services are also built for integration. You can use several AWS services together to provide the most secure environment for your data and resources.

AWS customers are able to tailor, or harden, the configuration of an EC2 instance, Amazon Elastic Container Service (Amazon ECS) container, or AWS Elastic Beanstalk instance, and persist this configuration to an immutable Amazon Machine Image (AMI). Then, all new virtual servers (instances) launched with this AMI receive the hardened configuration, whether they are launched manually or through automatic scaling.

Automate Security :

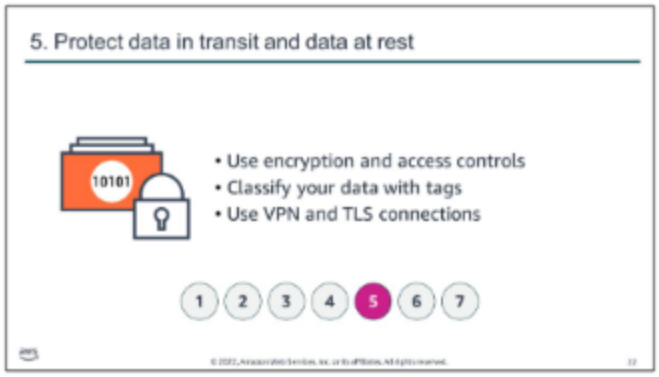


AWS develops purpose-built security tools that can help you to automate many of the routine tasks that security experts normally spend time on. This means the security experts can spend more time focusing on measures to increase the security of your AWS Cloud environment.

You can automate security engineering and operations functions by using a comprehensive set of APIs and tools. You can fully automate identity management, network security and data protection, and monitoring capabilities, and deliver them by using popular software development methods that you already have in place. Rather than having people monitor your security position and react to an event, with automation, your system can monitor, review, and initiate a response.

In the AWS Cloud, you can turn your infrastructure into code. With this capability, you can automate the creation of trusted environments to conduct deeper investigations and forensics. You can run incident response simulations and use tools with automation to increase your speed for detection, investigation, and recovery. By automating deployments and maintenance, you can remove operator access to reduce your attack surface area.

Protect data in transit and data at rest :



Safeguarding data is a critical piece of building and operating information systems. AWS provides services and features that help you to protect your data at rest and in transit. Safeguards include fine-grained access controls to objects, creating and controlling the encryption keys that are used to encrypt your data, selecting appropriate encryption methods, integrity validation, and appropriate data retention. To help you manage protection, implement a tagging schema to classify your data into sensitivity levels. Another security best practice is to construct mechanisms to protect data in transit, such as using virtual private network (VPN) and Transport Layer Security (TLS) connections.

AWS provides multiple means to encrypt data at rest and data in transit. We build features into our services that make it easier to encrypt your data. For example, we have implemented server-side encryption (SSE) for Amazon S3 to make it easier for you to store your data in an encrypted form. You can also arrange for Elastic Load Balancing (ELB) to handle the entire HTTPS encryption and decryption process (generally known as SSL termination).

Prepare for security events :

Even with mature preventive and detective controls, you should put processes in place to respond to and mitigate the potential impact of security incidents. The architecture of your workload strongly affects your ability to operate effectively during an incident, isolate or contain systems, and restore operations to a known good state. Put tools and access in place ahead of a security incident. Then, routinely practice incident response through game days. This will help you ensure that your architecture can accommodate timely investigation and recovery. Another module in this course will describe a variety of approaches to incident response.

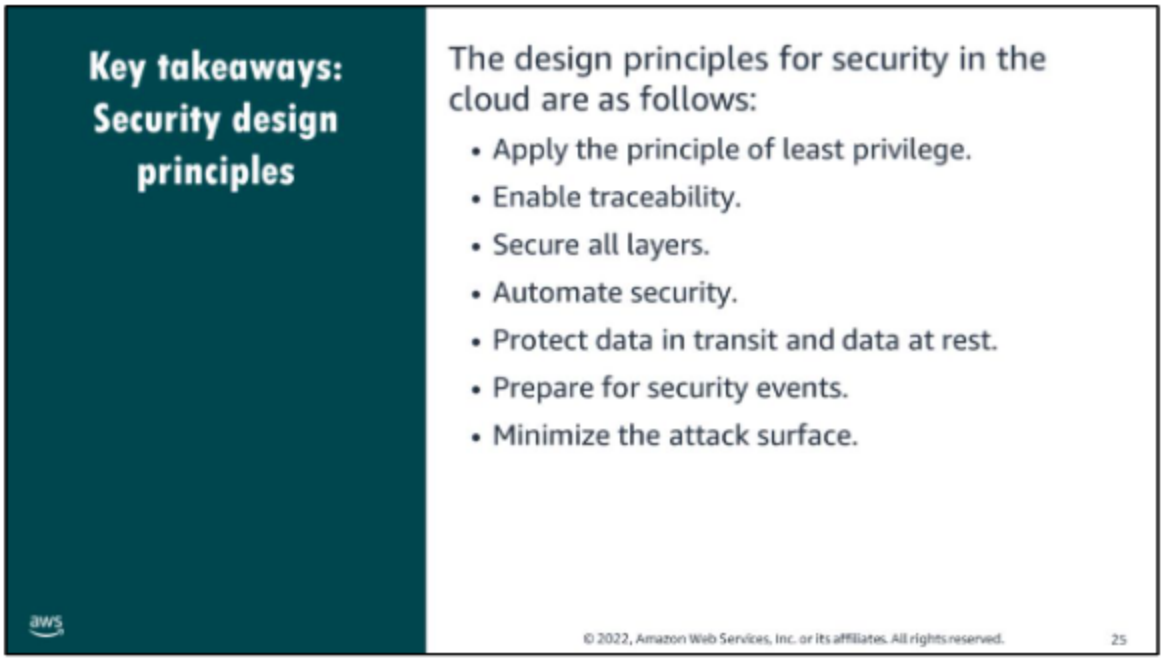
In AWS, the following practices facilitate effective incident response:

- Detailed logging is available. Logs contain important content such as file access and changes.
- Events can be automatically processed and invoke tools that automate responses through the use of AWS APIs.
- You can pre-provision tooling and a "clean room" by using AWS CloudFormation. This provides the ability to carry out forensics in a safe, isolated environment.

Minimize the attack surface :

Generally, a cyberattack shuts down due to two reasons: either the attackers exhaust themselves and give up, or the attackers achieve their goal. Reduce your exposure to unintended access by hardening operating systems and minimizing the components, libraries, and externally consumable services in use. Start by reducing unused components, such as operating system packages and applications. Configure security groups and network access control lists (ACLs) in Amazon Virtual Private Cloud (Amazon VPC) to help reduce the attack surface of your applications.

Certain AWS services, such as AWS Auto Scaling and Amazon CloudFront, help applications to scale to absorb common infrastructure layer attacks such as UDP reflection attacks and SYN floods. A UDP reflection attack takes place when the attacker asks the target computer for information by using a forged source address. A SYN flood is a type of distributed denial of service (DDoS) attack that aims to make a server unavailable to legitimate traffic by consuming all available server resources. By using techniques such as automatic scaling, you can absorb larger volumes of application layer attacks.



Shared Responsibilty Model

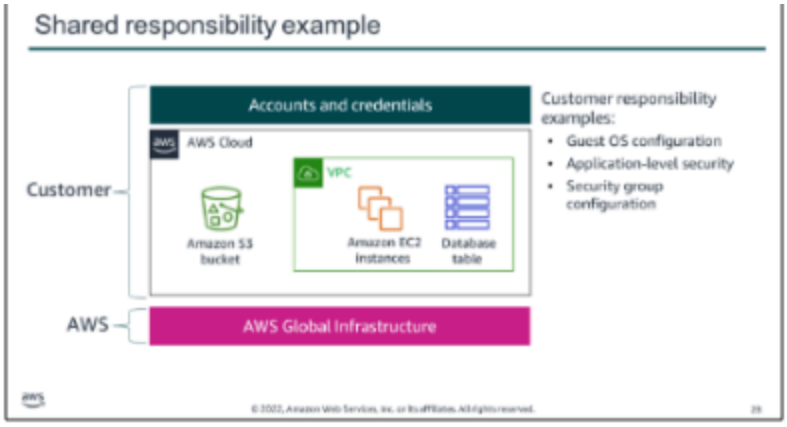
- Here, we'll go through the different models that we can use to share responsibility with AWS provider...

For accessibility: Shared responsibility model listing customer and AWS responsibilities. Customer is responsible for security in the cloud. This includes customer data. Platform, applications, identity and access management. Operating system, network, and firewall configuration. Client-side data encryption and data integrity, authentication. Server-side encryption of file system and data. Networking traffic protection, to include encryption, integrity, and identity. AWS is responsible for security of the cloud. This includes the AWS foundation services for compute, storage, databases, and networking. And the AWS Global Infrastructure, to include Regions, Availability Zones, and Edge Locations. **End of accessibility description.**

Security and compliance are shared responsibilities between AWS and customers. AWS operates, manages, and controls security *of* the cloud. This responsibility includes securing components, from the host operating system and virtualization layer down to the physical security of the facilities where the service operates. AWS is responsible for protecting the global infrastructure that runs all the services that are offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

- You assume responsibility and management in the cloud. The security steps that you must take depend on the services that you use and the complexity of your system. Customer responsibilities include selecting and securing operating systems that run on EC2 instances, and securing the applications that are launched on AWS resources. Customers must also select and handle security group configurations, firewall configurations, network configurations, and secure account management. Customers are also responsible for managing their data, including encryption options.
- To reiterate, AWS secures the hardware, software, facilities, and networks that run all AWS products and services. You are responsible for what you implement by using AWS products and services, and for the applications that you connect to AWS. The security steps that you must take depend on the services that you use and the complexity of your system.

- Here's an example :

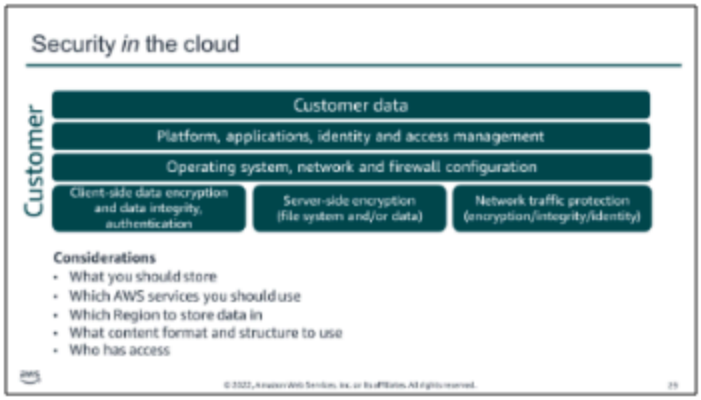


Consider an example where your company uses Amazon S3 to store data. Your AWS environment also includes EC2 instances and an Amazon Relational Database Service (Amazon RDS) instance. These resources run a MySQL database, which is deployed inside a virtual private cloud (VPC). One EC2 instance hosts a web server, and the web application that runs on it uses the database to store application data.

In this scenario, AWS is responsible for protecting the global infrastructure, which contains the physical servers that host the virtual machines and storage hardware. These virtual machines and storage hardware host your S3 bucket, EC2 instances, and database instance. AWS is responsible for the security of the physical networking infrastructure that ensures that these components can be accessed. AWS is also responsible for the security of the hypervisor layer that hosts the EC2 instances. (The hypervisor is the host OS that runs the EC2 instances, which are virtual machines that run guest operating systems.)

You (the customer) are responsible for managing the guest OS that runs on the EC2 instances (including Microsoft Windows or Linux OS updates and security patches). You are also responsible for managing any application software or utilities that you install. Additionally, you are responsible for the configuration of the security groups that control network access to each EC2 instance and to the RDS database instance. You are also responsible for configuring security on the S3 bucket and the objects that you store in it. For example, you could use one or more of the security features that AWS provides, such as bucket policies, data encryption, and S3 Block Public Access.

- Security in Cloud (Client side):



While AWS secures and maintains the cloud infrastructure, you are responsible for securing everything that you put *IN* the cloud.

Before you architect any workload, you need to put practices in place that influence security. You will want to control who can do what. In addition, you want to be able to identify security incidents, protect your systems and services, and maintain the confidentiality and integrity of data through data protection. You should have a well-defined and practiced process to respond to security incidents. These tools and techniques are important because they support objectives such as preventing financial loss or complying with regulatory obligations.

Because AWS physically secures the infrastructure that supports our cloud services, as an AWS customer you can focus on using services to accomplish your goals. The AWS Cloud also provides greater access to security data and an automated approach to respond to security events.

When using AWS services, you maintain complete control over your content and are responsible for managing critical security requirements, including the following:

- The content you choose to store on AWS
- The AWS services that are used with the content
- The country in which that content is stored
- The format and structure of that content, and whether it is masked, anonymized, or encrypted
- Who has access to that content, and how those access rights are granted, managed, and revoked

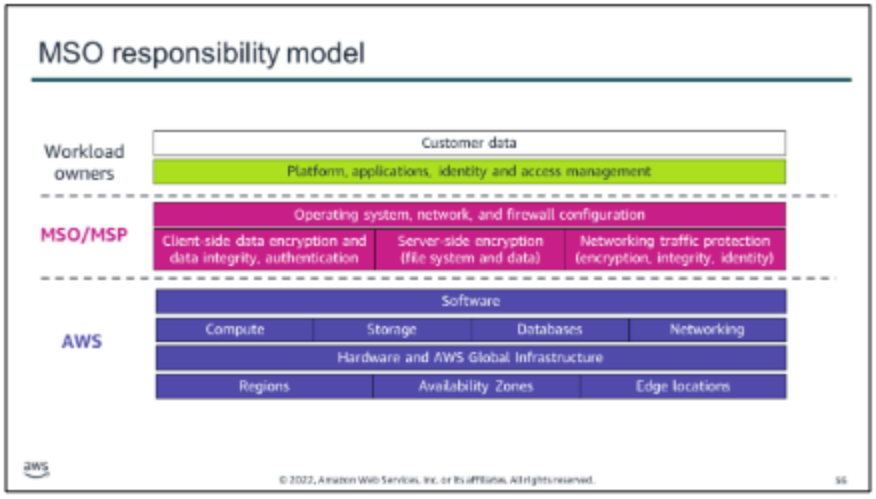
You retain control of what security you choose to implement to protect your own data, platform, applications, identity and access management, and operating system. This means that the shared responsibility model changes depending on the AWS services that you use.

MSO (Managed Services Organization)

- So basically, these are a team which don't belong to the client company nor AWS, they are a third party team that work 24/7 in providing security services in IT in general for that company...

One approach to implement security and governance is to create a centralized team that is responsible for establishing repeatable processes and templates to deploy applications to AWS while maintaining organizational control over the deployments. Such a team could be either internal or external (third-party vendors), and is often referred to as a provisioning team, center of excellence, or managed services organization (MSO). External vendors are commonly referred to as managed service providers (MSPs). AWS validates AWS Partners under the AWS Managed Service Provider (MSP) Program.

MSOs or MSPs are typically responsible for provisioning accounts; establishing repeatable processes for deployment; auditing the deployments of workload owners; and hosting shared services for security, continuous monitoring, connectivity, and authentication. MSOs essentially create the guardrails for security, data protection, and disaster recovery in the company.



In the MSO model, workload owners handle the actual deployment, development, and maintenance of applications. Workload owners typically include system administrators, developers, and others who are directly responsible for one or more applications. Adding an MSO helps ensure that applications are deployed in a secure and compliant fashion through the automated implementation of organizational security requirements. Having an MSO also means that the workload owner can scope down their authorization documentation to only the configuration and installation of software that is specific to a particular application. This is because the workload owner inherits a significant portion of the security control implementation from the MSO.

AWS customer MSOs often perform the following activities:

Account provisioning: After reviewing the workload owner's use case, the MSO establishes the initial account, connects it to the appropriate account for consolidated billing, and configures basic security functionality before

AWS customer MSOs often perform the following activities:

Account provisioning: After reviewing the workload owner's use case, the MSO establishes the initial account, connects it to the appropriate account for consolidated billing, and configures basic security functionality before granting access to the workload owner.

Security oversight: With centralized account provisioning, the MSO can implement features that enable security personnel to monitor the application as it is deployed and managed. The MSO might perform activities such as establishing an auditor group with cross-account access and linking the application VPC to a shared services VPC that the MSO controls.

Amazon VPC configuration: An Amazon VPC configuration includes the VPC and its subnets, security group configurations, and network access control lists (ACLs). To maintain tighter control over the application VPCs, the MSO might retain control of VPC configuration and require the workload owner to request wanted changes to network security.

IAM configuration: The MSO can create user groups and assign permissions. This can include creating groups for internal auditors, an IAM superuser, and application administrative groups that are segregated by functionality (for example, database and Unix administrators).