AWS

Introduction to AWS for Non-Engineers

Module 2 Security

Core concepts of cloud computing

- You probably heard of the cloud in the past few years, referring to ambiguous things that no one quite seems to define. You might have also heard of Amazon Web Services. Perhaps your company is considering utilizing it, or you're looking to find out more about this cloud computing platform that's taking the world by storm for your own career advancement. Whatever the reason may be that got you to click on this course, I'm glad you're here. I want to help you start from, What even is the cloud, to getting excited about Amazon Web Services, cloud computing, and potentially even consider taking the AWS Certified Cloud Practitioner exam. In Introduction to AWS for Non-engineers Two: Security, we will be focusing on security in the cloud and how it is similar and different from security in legacy IT infrastructure. We'll learn about security-related services offered through Amazon Web Services, and various security-related concepts that are important to keep in mind as you consider moving your resources onto the cloud. This course is also a vital part of your exam prep if you are thinking about taking the AWS Certified Cloud Practitioner exam. I can't wait to begin our cloud journey. Let's get started.

AWS Certified Cloud Practitioner exam

The AWS Certified Cloud Practitioner Exam is the only foundational level certification exam from Amazon Web Services, and requires no hands-on engineering experiences or prerequisite certifications. It validates the candidate's overall fundamental understanding of the AWS Cloud and basically serves to show your employers that you get what AWS does and how it operates to provide cloud computing services to its customers. While it is in no way required, it is a recommended stepping stone to taking the Associate or Specialty-level certification exams. AWS recommended that a candidate has six months of experience with the AWS Cloud in any role, ranging from technical, managerial, sales, purchasing, or financial before taking the certification exam. **But, from my experience and those of many others, this is not a strict necessity as long as the candidate has the fundamental knowledge necessary for the exam through studying.** Basic understanding of IT services and their uses in the AWS Cloud platform is also recommended. The certification exam is 90 minutes long and can be taken online or at the testing center. It costs 100 U.S. dollars per attempt and is available in English, Japanese,

Korean, and simplified Chinese. Unlike many other AWS certification exams, it has a hard pass score of 70% and is a multiple choice exam. So, what does the certification exam validate in terms of your knowledge and skills? The certification shows that you can define the AWS Cloud and the basic global infrastructure, describe basic AWS Cloud architectural principles and value proposition, and describe key services on AWS Cloud as well as common use cases. It also shows that you know the basic security and compliance aspects of AWS Cloud, and can define the billing, account management, and pricing models. The exam proves that you can describe the core characteristics of deploying and operating your IT infrastructure in the AWS Cloud. Finally, it shows that you can identify sources of documentations and technical assistance such as submitting support tickets and reading white papers.

Security domain

There are four domains in the AWS Certified Cloud Practitioner Exam. They are cloud concepts, security, technology, and billing and pricing. The four courses in the Introduction to AWS for Non-Engineers series follow these four domains. This course that you are watching now covers the second domain, the security domain, because securing the cloud by keeping your AWS Cloud infrastructure safe from both internal and external exploits is extremely important. The security domain is well worth your time to investigate.

There are four major points AWS wants you to be comfortable with before taking a Certified Cloud Practitioner Exam. They want you to define the AWS shared responsibility model and AWS Cloud security and compliance concepts. They also want you to identify AWS access management capabilities and also be able to identify resources for receiving security related support. We will review different security related concepts, like the shared responsibility model, security pillar of the well-architected framework, principle of least privilege, and AWS Cloud compliance. Ever wonder what it means to quote/unquote secure the cloud? We will also talk about what it means to secure the cloud, which could be a little different or similar to securing your on-premises IT infrastructure in a data center. In addition, we will review some major security related AWS services, like AWS Identity Access Management or IAM, AWS Web Application Firewall, or WAF, and AWS Trusted Advisor amongst other core security services. We'll provide study breaks and exam study tips so you can begin preparing for the AWS Certified Cloud Practitioner Exam security domain. Ready to get started? Let's go.

Security in the cloud

Security in the Cloud. If you're anything like me, when you think about security for your data and your IT infrastructure, you probably think of the server room in your office, locked with a card key that only the IT department has. Or maybe your company has a data center off-site that you have to drive two hours to get to, to make sure your backups are being saved securely. When

you get to the data center, you probably encounter a lot of security personnel and need to submit a lot of credentials to step into the facility and get anywhere near the servers. This image of securing data is quickly being replaced by cloud-based security where you no longer have to keep costly data centers functioning and secured. Instead, you can have a cloud computing service provider manage their own data centers on your behalf so you can focus on other aspects of IT infrastructure management. When you deploy your IT resources into AWS Cloud, you benefit from the global network of data centers and architecture built with security in mind. AWS helps you keep your data safe in their highly secure data centers, and there are safeguards in place to help protect customer privacy. There are dozens of compliance programs embedded into AWS to help you meet your industry's compliance requirements for data security. Securing your data on AWS Cloud allows you to maintain the highest standard of security without having to manage your own data centers, which saves you time and money. It also allows you to scale the size of your business quickly, as AWS is designed to keep data safe no matter how big or small your cloud usage is. Let's learn about a few concepts and frameworks for security in the cloud before discussing specific security-related services that AWS offers.

Shared responsibility model

When utilizing the cloud to house any part of your technical infrastructure, you must first consider the security impacts of moving your resources onto the cloud. Unlike the on-premises data center that is protected by the virtue of being within your physical reach, data centers hosting your cloud resources are in an undisclosed location in data centers managed by AWS. So who's responsible for the security of the data center? The servers? The networks? The data itself? All those EC2 instances that are running computations. Who makes sure their security patches are up to date? Who protects the data from being corrupted? AWS has a model that helps to puzzle these questions out, called the Shared Responsibility Model. As you might expect from the name, the Shared Responsibility Model asserts that the security of cloud functioning infrastructures is a shared responsibility between the customer and AWS. While there are certain parts of the infrastructure that the customers no longer have to worry about, there are still components that are the customer's responsibilities to secure.

In the most basic breakdown, AWS is responsible for the security of the cloud, while you, the customer, are responsible for security in the cloud. Let's see if we can deconstruct what AWS might mean by this. When AWS says that they are responsible for security of the cloud, they mean that AWS is responsible for protecting the infrastructure that runs all of the services offered by AWS Cloud. This includes hardware, software, networking and the data center facilities that run their cloud computing platform. You can think of it like, AWS is responsible for security of the components that make up the AWS Cloud, like the data centers and physical servers. On the other hand, when AWS says that the customers are responsible for security in

the cloud, they mean that the customers are responsible for varying levels of security functions, depending on which services they are using. These could be in forms of protecting customer data, platform, application, and identity or access management. Or operating systems of virtual machines, configuring firewalls and data encryption. You can think about it like, we are responsible for the security of things inside the AWS Cloud, like data encryption and patching servers. There are many granular settings and concepts within the Shared Responsibility Model for AWS Cloud, which you can read on their website. But the basic concept that you need to know for the exam when this model is brought up is this, AWS is responsible for security of the cloud, while you, as the customer, are responsible for security in the cloud.

Well-architected framework

- Security in a Well-Architected IT infrastructure. When you're considering architecting how your AWS cloud IT infrastructure will look, you will have to put in a lot of considerations on how to make sure that it is secure from both external and internal threats. AWS has developed the concept called the five pillars of a well architected framework to help you build the most secure, fault resilient, efficient and high performing IT infrastructure possible. The pillars are discussed in detail in the first course of this series titled Introduction to AWS for non engineers, one cloud concepts. Since this course pertains to security, we'll be doing a deeper dive into you guessed it, the security pillar. They are Identity and Access Management or IAM, Detective Controls, Infrastructure Protection, Data Protection and Incident Response. To make sure user access is manage properly, you would want to implement a strong identity foundation. This would entail utilizing the principle of least privilege, which means that you only provide access to what people need to do their jobs, and no more. We will go over this concept in more detail in the next video.

You should enable traceability by monitoring alerts, audit actions and changes to your environment in real time. Security should be applied on all layers instead of just on a single outer layer of your infrastructure. For a virtual server, this could mean that you make sure your infrastructure is secured at the organizational subnet, load balancer virtual machine in the operating system layers. Security best practices should also be automated, so that you can scale more rapidly and cost effectively. If the security methods are automated, You can just replicate that for every new instance or resource you deploy instead of having to manually set them up. Data should be protected At Rest and In Transit data is At Rest when it is stored somewhere like in an S3 bucket. Data is In Transit when it is moving from one place to another, such as when you send an email from your mail server to your friend's mail server. Security mechanisms should be adjusted depending on sensibility of the data. You should also keep people away from the data by eliminating the need for direct access or manual processing of data. In this way, human error and loss or modification of sensitive data can be prevented. Finally, when a security event occurs, you should be prepared to intervene, investigate and deal with the event. And once the issue is resolved, update the incident

management process to learn from the security event. Security is a very vital part of running and architecting a well architected framework. You can strive for stability by focusing on protecting the data and resources against security events. And when an event occurs to learn from the event and update Incident Management procedures.

Principle of least privilege

Principle of least privilege. Who can access what? When you start a new job, you get some accounts to log in. It can be your not so new computer with someone else's coffee stains on the keys, or your corporate email account that has fifty emails waiting for you already. Or, it could be your company's shared network drive on the server, where your team and your predecessors have been keeping documents that everyone needs to access. Say you work in the sales departmnet. You should have access only to resources and information that you require to do your job. That could be the client list for your team, or deck templates for slideshows you will now be creating to present to potential clients. Or, even the products you are selling, however, you will not expect and should not have access to resources like pending legal cases being handled by the legal department, the not-yet released product mock-ups being developed by your dev teams, or list of personnel reshuffling that the HR department is contemplating.

This concept of providing access only to resources that a person needs to do his job, and no more, is called the principle of least privilege. The concept is this. The CEO of the company should have access to a lot of the corporate resources. The newly hired sales associate should not. The IT department should have the ability to administer the services, but probably not have access to the sensitive information and files themselves. Every role has a set of access permissions necessary to effectively complete its job, and the individual in the role should have no more or no less than the optimal level of access.

To follow the principle of least privilege in AWS, you provide access to services and resources for your users and other AWS services by using a service called Identity Access Management, or IAM. When you provide users or services access using IAM policies you should start with a minimum set of permissions and grant additional permissions only as necessary. Determine what the user or service needs to be able to do and craft policies to allow them to perform only those specific tasks. For example, a marketing manager might need to access certain marketing-related S3 bucket to upload flat files for the company's website. You may remember that S3 is a file store service offered by AWS, and buckets are like folders inside the service that holds your files. However, he will not need access to the S3 buckets where air logs are being dumped into by an app being developed by the dev team. The IAM access granted to the marketing manager should provide him only the absolute necessary access in the company's AWS cloud infrastructure. Remember to provide only the minimum amount of access a person or service requires and nothing more to keep your AWS cloud infrastructure secured.

AWS Cloud compliance

AWS has many compliance programs available for your review in order to determine whether your industry allows you to store data or use AWS for your business. You can find the AWS Compliance Programs by going to aws.amazon.com/compliance/programs. Let's take a look together. Here, we can see that the AWS Compliance Programs are divided up into regions of the world. There's also a whole entire section on privacy. That's definitely a big one for the data on the cloud. If your organization deals with patient data in the United States, you would need to be cognizant of HIPAA. You can find out how AWS is compliant with HIPAA and how data is secured on AWS. Let's take a look. Let's see, here we go. Laws, regulations, privacy, HIPAA. If you had any questions, the quick FAQ will respond to many of the common questions. There are many compliance programs available for review. And this page allows you to easily find out whether your resources can or cannot be hosted on AWS if you have compliance requirements for your data. Again, you can find the information on aws.amazon.com/compliance/programs.

Study break: Security domain

What are the differences between security in the Cloud and security in an on-premises data center? Security in the Cloud may look a little different, and include some added benefits. Let's review the security domain of the AWS Certified Cloud Practitioner Exam together. Some topics we'll be covering are the security in the Cloud, Shared Responsibility Model, security pillar of the Well-Architected Framework, Principle of Least Privilege, and AWS Cloud Compliance. Let's go.

One of the biggest benefits of utilizing Cloud computing is that you no longer have to purchase equipment and maintain your own data center to run IT resources. Cloud computing providers like AWS manage the data centers so you can focus on other aspects of IT infrastructure management. When you deploy to the AWS Cloud, you benefit from the global network of data centers and architecture built with security in mind. There are dozens of compliance programs embedded into AWS to help you meet your industry's compliance requirements. AWS is designed to keep your data safe, no matter how big or small your Cloud usage is, so you are free to scale your business as quickly as you want.

There are three major concepts that outline AWS' recommended security practices. These are: the Shared Responsibility Model, the Security Pillar of a Well-Architected Framework, and Principle of Least Privilege. In addition, we will review how AWS accounts for compliance requirements for data and resources stored in the Cloud. The first concept addresses the question who is responsible for security? The answer is slightly complex. You, as the consumer, are responsible for security in the Cloud. AWS, as the Cloud computing service provider, is responsible for security of the Cloud. This concept is called the Shared Responsibility Model, and it asserts that the security of the data and resources in the Cloud is a shared responsibility between the Cloud computing service provider and the customer. While the

customer no longer has to worry about certain aspects of IT infrastructure, like securing the physical data center or hardware, there are other aspects that they are still responsible for, including patching virtual service regularly, and utilizing proper permission sets so only people who should be accessing certain resources, do access them.

Next, AWS addresses how can you best protect your AWS Cloud infrastructure from both internal and external security threats? AWS has the five pillars of a Well-Architected Framework to help it's customers build the most secure, fault resilient, efficient, and high performing IT infrastructure possible. Within the five pillars, there is the security pillar, which outlines how you can secure your infrastructure adhering to best practices. Security in the Cloud is composed of five areas: Identity and Access Management, Detective Controls, Infrastructure Protection, Data Protection, and Incident Response. Architecting a Well-Architected Framework can go a long way to making your IT infrastructure stable and secure.

Next is Principle of Least Privilege. What resources should you provide access to? The Principle of Least Privilege states that you should only be providing access to resources that an entity requires to do it's job. Every role has a set of access permissions necessary to effectively execute it's job, and the resources and individuals should have no more or no less than the optimal level of access. In AWS, you would make this happen by using a service called Identity and Access Management, or IAM, providing granular access permissions. Providing the minimum amount of access to entities to complete their work is a vital way to keep your IT infrastructure secure. The Principle of Least Privilege coincides with the Shared Responsibility Model, where the customer, you, are responsible for security in the Cloud by making sure access is provided responsibly.

Lastly, here are many AWS Cloud Compliance programs available to help you determine if your industry allows you to store data on AWS. Many industries have compliance requirements for storing your data, such as HIPAA for medical organizations. You can learn more about the various compliance programs AWS offers by visiting aws.amazon.com/compliance. In the security domain of the AWS Certified Cloud Practitioner Exam, AWS wants you to be able to explain what concepts like the Shared Responsibility Model and Principle of Least Privilege may mean in real life scenarios. If you feel like you want or need a refresher for any of the concepts we reviewed in this video, feel free to go back and watch the videos again.

Identity and Access Management (IAM)

When utilizing the cloud to house any part of your technical infrastructure you must first consider the security impacts of moving your resources onto the cloud. Unlike the on-premises data center that is protected by the virtual being within your physical reach, data centers hosting your cloud resources are in an undisclosed data centers managed by AWS. By now you've probably surmised it's not the best idea to provide unrestricted access to your IT resources to everyone in your organization, but is there an easy way to provide extremely

granular access permissions to every user in service but at the same time make them easy to manage? Thankfully, AWS has a service called Identity Access Management commonly referred to as IAM which helps you do just that.

Identity and Access Management, or IAM, is a free service provided by AWS that enables you to manage access to services and resources on the AWS cloud. You can create and manage users and groups as well as set permissions to allow or deny access to various resources. The permissions are global which means that the access you set for a user or group will be true for all regions in AWS Cloud. When providing access to users and services you should follow the principal of least privilege. There are a few ways you can set permissions for various services or users to access your AWS resources. You can use IAM to manage users, manage roles and manage federated users. The first way you can set access is by using IAM to manage users. You can create users in IAM and assign them individual security credentials. These users can have very granular permission sets so you can control which operations a user can perform on which specific service. A user could be administrators that need console access to manage the AWS Cloud account, end users who need to access content in the AWS Cloud account or systems that need the ability to programmatically access data in the AWS Cloud account. Programmatic access means that applications are directly accessing resources in the AWS Cloud as opposed to humans doing the same activity. Another way to set access is to manage IAM roles. You can create roles to manage permissions and control what these roles can do in your AWS instance.

An entity assumes a role and can obtain a set of temporary security credentials to make API calls to your AWS resources. This could be used to provide access to a user from another AWS account to your AWS account such as when an organization has separate develop and production environments. The last way to set access is to manage federated users. By enabling identity federation you can allow existing identities in your enterprise to access your AWS cloud instance without having to create an IAM user for each user. You can use any identity management solution that supports SAML 2.0 or use one of AWS's federation samples. You've probably experienced identity federation in action when you sign up for an online service using your Facebook or Gmail account. In a corporate setting you could have your Microsoft Active Directory users have federated access to your AWS cloud instance using identity federation. Some benefits of IAM are enhanced security, granular control, ability to provide temporary credentials, flexible security credential management, ability to leverage external identity systems using federated access and seamlessly integrating various AWS services within the AWS Cloud infrastructure.

Web application firewall (WAF)

Web Application Firewall or WAF. AWS Web Application Firewall, commonly referred to AWS WAF, protects web applications running on AWS Cloud from common web exploits. As the

name suggests, it's a firewall service for your web applications. Fancy that. WAF can protect against exploits that could compromise security or availability of your web apps. It can also protect the application from exploits that could force your app to consume excessive resources which in turn could end up costing you a lot of money. With WAF, you only pay for what you use with no upfront commitments. Web Application Firewall improves web traffic visibility, provides cost-effective web application protection, and delivers increased security and protection against web attacks. It is also easy to deploy and maintain, as you can deploy it on Amazon CloudFront as part of your content delivery network solution or via Amazon API Gateway. There is no additional software that you need to deploy and you can reuse the centrally-defined roles across all of your web applications. AWS WAF is an affordable, malleable, and adaptable protection for your web applications running on AWS Cloud that is easy to manage and deploy.

Shield

AWS Shield. Have you ever experienced Distributed Denial of Service or DDoS attacks, you might have tried to access your favorite social network platform, only to find that the website is glitchy, or nothing is loading on your browser? You might Google the website or complain about it on another social media network. And you might find out that the website is experiencing a DDoS attack. A Distributed Denial of Service Attack or DDoS attack is an attempt to make a machine or network resource unavailable temporarily or indefinitely, most often by making excessive repeated access requests to the website using thousands of unique IP addresses. Basically, a hacker or malicious personal organization would overload the server with access requests so that real users can't access the website because it's to busy.

Have you ever felt extremely overwhelmed by multiple requests coming from all different places? Maybe you worked on extremely busy restaurant when a coworker called out or you had multiple project deadlines at the office while some dumpster fire was going on, that you needed to fix, you likely felt overwhelmed, exhausted and unsure how to deal with the workload. And perhaps you mentally shut down unable to process all the different requests. This is what happens to the servers when it's under a DDoS attack.

AWS has a service called AWS Shield, which provides detection and automatic mitigations to minimize the effects of DDoS attack on your applications. AWS Shield helps to minimize application downtime and latency when an attack happens. There are two tiers to AWS Shield in terms of protection and cost. The standard tier is automatically enabled, free to use and protects your web application against majority of common DDoS attacks. When used with CloudFront and Route 53. You can obtain comprehensive availability protection against all known infrastructure attacks. The second tier is called Shield Advanced and it provides 24/7 access to the AWS DDoS response team. It detects and mitigates sophisticated DDoS attacks with near

real-time visibility into the events and integrates with AWS WAF. Shield Advanced provides higher level protections, network and transport layer protections and automated application traffic monitoring. Shield Advanced also provides financial protection against DDoS related spikes for charges for EC2, elastic load balancers, CloudFront and Route 53. It is available globally on all CloudFront and Route 53 Edge locations. This means that your web application can be hosted anywhere in the world but still be protected by AWS Shield as long as you're able to deploy CloudFront instance in front of the server. With two-tiered support, AWS Shield can provide comprehensive protection against DDoS attacks small and large that is catered to your budget and needs. If you have a small product, you can get started with the standard protection and as it scaled, you can upgrade your protection to suit your needs.

Inspector

Amazon Inspector. If you or your company develops applications, there's a service that can provide your auditors and your development team a peace of mind knowing that the applications adhere to security standards set by the company and the industry as a whole. Amazon Inspector is an automated security assessment service for your applications deployed on AWS. This means that it helps you improve the security and compliance of these applications by automatically assessing them for exposure, vulnerabilities, and derivations from best practices. Once the assessment is completed, it generates detailed reports to help you check for unintended vulnerabilities. Security teams can then get reports validating that tests were performed. Inspector helps you reduce the risk of introducing security issues during deployment and development by proactively identifying potential issues that do not align with best practices and policies. You can define your own standards and best practices, and make sure that they're being followed. Or you can choose to utilize AWS's constantly updated standards. As the name suggests, Amazon Inspector inspects your applications to find security issues and bring them to your attention.

Trusted Advisor

AWS Trusted Advisor. Have you ever looked at your finances and thought, "Well dang. "I wish someone would tell me what to do with my money, "so I could have a comfortable early retirement?" I've tried some investments, I've tried putting money into a 401k, but I have no idea if I'm doing any of this right. Oftentimes, the people you call up about your money health are called financial advisors. For your AWS Cloud infrastructure, you have Trusted Advisor.

AWS Trusted Advisor is a service that guides the provisioning of your resources, so that you are following AWS best practices. Upon scanning your AWS infrastructure, Trusted Advisor advises you on how your infrastructure is or is not following AWS best practices based on five categories. The categories are cost optimization, performance, security, fault tolerance, and service limits. AWS then provides action recommendations to bring your infrastructure closer to

best practice standards. All AWS customers have access to seven core trusted advisor checks for free. These checks are S3 bucket permissions, security groups, specific ports unrestricted, IAM use, MFA on root account, EBS public snapshots, RDS public snapshots, and service limits. For those with enterprise or business support plans, there are extended set of checks and recommendations available. On top of more types of checks, those with full trusted advisor access also get notifications through weekly updates, an ability to set up automated actions in response to alerts with Amazon CloudWatch. They also have programmatic access to the scan results via AWS Support API. AWS Trusted Advisor is a valuable ally in making sure that deployment of your AWS Cloud resources are aligned with best practices, as well as providing you customized recommendations based on proactive monitoring of your infrastructure.

GuardDuty

Amazon GuardDuty. In a perfect world, you wouldn't need to sleep so that you can be up at all times of the day and night monitoring your cloud infrastructure for threats and malicious activities. Unfortunately, we all need sleep, and some departments don't have the budget to have people staring at dashboards 24/7. Thankfully, you don't have to, because AWS Cloud has a service that stays up all day and night for you. It's called Amazon GuardDuty, and it's a threat detection service that monitors for malicious activity and unauthorized behavior to protect your AWS Cloud instance 24/7. It analyzes billions of events across multiple AWS data sources which can then send actionable alerts via AWS CloudWatch events. GuardDuty uses machine learning, anomaly detection, and integrative threat intelligence to identify and prioritize potential threats that may impact your AWS Cloud infrastructure. Best of all, you can deploy GuardDuty within a few clicks as there is no additional software or infrastructure to manage to take advantage of that protection. Amazon GuardDuty continuously monitors your AWS Cloud infrastructure, intelligently detects threats using machine learning and helps you take action immediately if a threat is found so that you and your team can have a good night's sleep knowing your infrastructure is being monitored at all times.

Study break: Reviewing security services

- Welcome to the Study Break. Let's review the security related services that may be relevant to the AWS Certified Cloud Practitioner exam. The security services we will be reviewing in this video are; AWS Identity and Access Management or IAM, AWS Web Application Firewall or WAF, AWS Shield, Amazon Inspector, AWS Trusted Advisor, and Amazon GuardDuty.

First, AWS Identity and Access Management, more commonly referred simply as IAM, is a free service that enables you to securely manage access to services and resources in the AWS cloud. The permission sets are extremely granular, helping you allow or deny access by users or other services to various resources. You can set access by using IAM to manage users utilizing granular permission sets. You could also create and manage IAM roles which has specific

permission sets. You can allow entities to assume a role to do specific actions in your AWS cloud instance. In this way, you don't have to manually set up every entities permission sets, which could result in human errors and inconsistencies.

Finally, you can enable identity Federation, which will allow existing identities in your enterprise accounts. Many organizations allow identity Federation for their Microsoft active directory. Allowing employees to access their AWS cloud instance without having to create a new IAM user for every single employee. IAM allows you to have enhanced security, granular control over permission sets, ability to provide temporary credentials, flexible security credential management, inability to utilize identity Federation.

Second, the AWS Web Application Firewall of WAF, is as it sounds. A firewall service for web applications running on AWS cloud. It protects web apps from common web exploits as well as potential compromises that could force your apps to consume excessive AWS resources, which could be detrimental to your finances. It improves web traffic visibility, provides cost-effective web application protection and delivers increased security against web attacks. It's an affordable protection for your web applications that can be deployed within minutes.

Another security service is AWS Shield, which can protect your web applications from a distributed denial of service or DDoS attack. It provides detection and automatic mitigation of DDoS attacks to applications, helping you minimize the negative consequences and application downtime. There are two tiers available for customers. The standard tier is automatic, free and protects web apps against majority of common DDoS attacks. The shield Advanced tier provides 24/7 access to AWS DDoS response team and detects and mitigates sophisticated DDoS attacks with near real time visibility into events. And even provides financial protection against DDoS-related spikes in AWS resource usages. You can receive comprehensive DDoS protection catered around your budget and needs with AWS shield.

Next, the Amazon Inspector is an automated security assessment service for your AWS applications, which helps you improve security and compliance. It inspects your applications automatically assessing them for exposure, vulnerabilities, and derivations from best practices. After an assessment is completed, it generates detailed reports to help you check for vulnerabilities. Utilizing Amazon Inspecter helps to reduce the risk of introducing security issues by proactively identifying potential security vulnerabilities that do not align with best practices and policies. You can define your own standards to check against and create reports that validate that specific tests were performed.

You can continue enforcing best practices within your AWS cloud infrastructure. What the help of AWS has constantly updated standards made available through inspector. Another crucial security service is the AWS Trusted Advisor, AWS trusted advisor guides provisioning of resources to AWS cloud. So you're following AWS best practices. As the name suggests, it advises you on how your infrastructure is or is not following AWS best practices based on five categories; Optimization, Performance, Security, Fault tolerance and Service limits. It then offers

recommendations to bring your infrastructure closer to standards. The Seven core Trusted Advisor checks are free and those with Business Support plans and above have access to Full Trusted Advisor checks. AWS trusted advisor provides customized recommendations based on proactive monitoring to make sure your AWS cloud deployments are aligned with best practices.

Lastly, Amazon GuardDuty is a threat detection service that monitors for malicious activity and unauthorized behavior 24/7. Utilizing machine learning, anomaly detection and integrated threat intelligence. GuardDuty identifies and prioritizes potential threats that may impact your AWS infrastructure. It's deployable with just a few clicks and helps you take action immediately against the threat. It works as a 24/7 monitoring solution to help your human infrastructure team get a good night's rest.

So, this was a quick study break review of the security related services AWS offers to help protect your cloud infrastructure. If you are unsure about your understanding of any, feel free to go back to the individual videos to get more in depth summaries of each, before moving on.

Study break: Exam tips and resources

Feeling ready? Let's go over some exam tips to help you prep for success. In this video, we will be going over contents that will be relevant to the security domain of the AWS Certified Cloud Practitioner exam. We will go over the shared responsibility model, principle of least privilege, security pillar of a Well-Architected Framework, and the security services. Let's get started.

The security domain is concerned with how to make sure your IT infrastructure hosted on AWS Cloud, is safe from both internal and external security threats. There are a few concepts related to this, such as the shared responsibility model, the security pillar of the Well-Architected Framework, and the principle of least privilege. In the shared responsibility model, the most important concept to understand is that you as the customer, and AWS as the cloud computing service provider, share the responsibility of keeping AWS Cloud secure. Customers are responsible for security in the cloud and AWS is responsible for security of the cloud. How do you make sure you're keeping the information in the cloud secure? You should only provide the least amount of access possible for any entity to make sure that no one has access to resources they are not entitled to. This concept is called the principle of least privilege.

Finally, the security pillar of the Well-Architected Framework states that the security of the cloud is composed of identity and access management, detective controls, infrastructure protection, data protection, and incident response. We also went over a few core security related AWS services such as AWS Identity and Access Management, or IAM, AWS Web Application Firewall, or WAF, AWS Shield, Amazon Inspector, AWS Trusted Advisor, and Amazon GuardDuty. You

should be familiar with what each of these services do and how they contribute to helping keep AWS Cloud secure. If you are unsure about any of the concepts or services we just discussed, feel free to check back on the videos, or even the study break videos to review. A few extra minutes making sure you have the services or concepts straightened out could mean a few extra points on the certification exam.