AWS Shared Responsibility Model

EBOOK

aws partner network

Table of contents

Security at the heart of your business

Cybersecurity poses a big risk for companies today. Without expert guidance, it can be challenging to know how to secure your IT environment.

Amazon Web Services (AWS) places security at the heart of every offering to help you fully realize the speed and agility of the cloud.

Our dedicated team of engineers works to constantly evolve our security services through core capabilities such as identity and access management, logging and monitoring, encryption and key management, network segmentation, and standard DDoS protection, as well as advanced areas like proactive threat detection.

AWS and the AWS Partner Network (APN) make it easy to tailor your security to meet the requirements of your business as you grow. AWS Security Competency Partners offer fully vetted solutions and services that work within the well-architected security of AWS to protect your unique environment.

The Shared Responsibility Model

Security is a shared responsibility between you and your cloud provider.

The AWS Shared Responsibility Model (SRM) makes it easy to understand your choices for protecting your unique AWS environment, and it provides you with access to resources that can help you implement end-to-end security quickly and easily.

AWS provides **Security of the Cloud** which protects the hardware, software, networking, and facilities that run your selected AWS Cloud services.

You control your **Security in the Cloud** which includes updating and patching the guest operating system, associated application software, and configuration of the AWS provided security group firewall.

The AWS Partner Network offers access to a large ecosystem of Security Competency Partners who can help you fulfill your security responsibilities through solutions and consulting services.

The Shared Responsibility Model empowers you with the clarity, flexibility, and control you need to build on the cloud with the utmost confidence.

The Shared Responsibility Model

Customers have their choice of security **IN the Cloud**

- CUSTOMER DATA
- PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
- OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
- CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
- SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
- NETWORKING TRAFFIC PROTECTION (ENCRYPTION INTEGRITY, IDENTITY)

aws competency

AWS is responsible for the security **OF the Cloud**

- SOFTWARE
  - COMPUTE
  - STORAGE
  - DATABASE
  - NETWORKING
- HARDWARE/AWS GLOBAL INFRASTRUCTURE
  - REGIONS
  - AVAILABILITY ZONES
  - EDGE LOCATIONS

AWS offers a wide range of certifications and attestations, covering compliance programs from around the globe. Learn more here.

Security is our top priority

AWS offers both a secure cloud computing environment and innovative security services that satisfy the security and compliance needs of the most risk-sensitive organizations.

With AWS and AWS Security Competency Partners, you can transform the way you do business, automating security and compliance tasks to reduce risk so you can grow and innovate faster, freeing up resources to focus on your customers and core business needs.

Build with the highest standards for privacy and data security

AWS is vigilant about your privacy. With AWS, you can build on a secure global infrastructure, knowing you always own your data, including the ability to encrypt it, move it, and
manage retention.

We provide tools that allow you to easily encrypt your data in transit and at rest to help ensure that only authorized users can access it, using keys managed by our AWS Key Management Service (AWS KMS) or managing your own encryption keys with AWS CloudHSM using FIPS 140-2 Level 3 validated HSMs.

We also give you the control and visibility you need to help demonstrate that you comply with regional and local data privacy laws and regulations. The design of our global infrastructure allows you to retain complete control over the regions in which your data is physically located, helping you meet data residency requirements.

We have a world-class team of security experts monitoring our systems 24x7 to protect your content.

Scale securely with superior visibility and control

With AWS, you control where your data is stored, who can access it, and what resources your organization is consuming at any given moment. Fine-grain identity and access controls combined with continuous monitoring for near real-time security information ensures that the right resources have the right access at all times, wherever your information is stored.

Reduce risk as you scale by using our security automation and activity monitoring services to detect suspicious security events, like configuration changes, across your ecosystem. You can even integrate our services with your existing solutions to support existing workflows, streamline your operations, and simplify compliance reporting.

Automate and reduce risk with deeply integrated services

Automating security tasks on AWS enables you to be more secure by reducing human configuration errors and giving your team more time to focus on other work critical to your business. Select from a wide variety of deeply integrated solutions that can be combined to automate tasks in novel ways, making it easier for your security team to work closely with developer and operations teams to create and deploy code faster and more securely.

For example, by employing technologies like machine learning, AWS enables you to automatically and continuously discover, classify, and protect sensitive data in AWS with just a few clicks in the AWS Management Console.

You can also automate infrastructure and application security checks to continually enforce your security and compliance controls and help enable confidentiality, integrity, and availability at all times.

Automate in a hybrid environment with our information management and security tools to easily integrate AWS as a seamless and secure extension of your on-premises and legacy environments.

Select from the largest ecosystem of security partners and solutions

Extend the benefits of AWS by using security technology and consulting services from familiar solution providers you already know and trust. We have carefully selected providers with deep expertise and proven success securing every stage of cloud adoption, from initial migration through ongoing, day-to-day management.

Choose from our AWS Partner Network (APN), a global program of Technology and Consulting Partners, many of whom specialize in delivering security-focused solutions and services for your specific workloads and use cases. APN Partner solutions enable automation and agility and scaling with your workloads.

These solutions work together to help secure your data in ways not possible on-premises, with solutions available for a wide range of workloads and use cases.

Partners and the AWS Marketplace

When it comes to your cloud security, there's no reason to go it alone. AWS has you covered every step of the way from Security of the Cloud managed by AWS engineers to our extensive network of partners who can help you handle Security in the Cloud.

Security is a shared responsibility. Build confidently on AWS.

The AWS Partner Network (APN) offers services and solutions that enable automation and agility, scale with your workloads, and help you keep your operational costs low.

Easily find, buy, deploy, and manage these cloud-ready solutions, including software as a service (SaaS) products, in a matter of minutes from the AWS Marketplace.

For more information, visit aws.amazon.com/partners and aws.amazon.com/marketplace

About CloudLink.

CloudLink helps the healthcare industry's customers implement migrations, enhance security and reduce costs by successfully Following:

1. Offshoring Business model ;
2. IT security management's best practices; (ISO 27001)
3. Project management best practices;
4. Matching the customers' time zone;
5. Reducing costs.

On the AWS Cloud, customers can take security a step further by adopting the log management and compliance's best practices in accordance with the HIPAA and the HITECH Act regulations. At CloudLink we prioritize our customers by offering reduced costs instead of the overpriced consulting fees you usually find.

CloudLink case study: Software Business

Challenge

Security is an essential element of any application especially when it comes to the Restful API layer. Thousands of calls are made daily to share information via Rest APIs, making security a top concern for all organizations in all stages: designing, testing, and deploying the APIs. We are living in an era where our private information is more vulnerable than ever before, so it is very important to protect your APIs from threats and vulnerabilities that keep on increasing daily.

In addition to all the guidelines available for building a secure API, an important step is to make your API private. Attackers will not be able to launch any attack on your API if they cannot find it. Exposing your APIs to the public will add a range of security and management challenges that you can avoid. While it is easy to spin up simple these cloud architectures, mistakes can easily be made provisioning complex ones. Human error will always be present, especially when you can launch cloud infrastructure by clicking buttons on a web app.

The only way to avoid these kinds of errors is through automation, and Infrastructure as Code is helping engineers

automatically launch cloud environments quickly and without mistakes.

CloudLink case study: Software Business

Solution

Architecture - 1st Phase

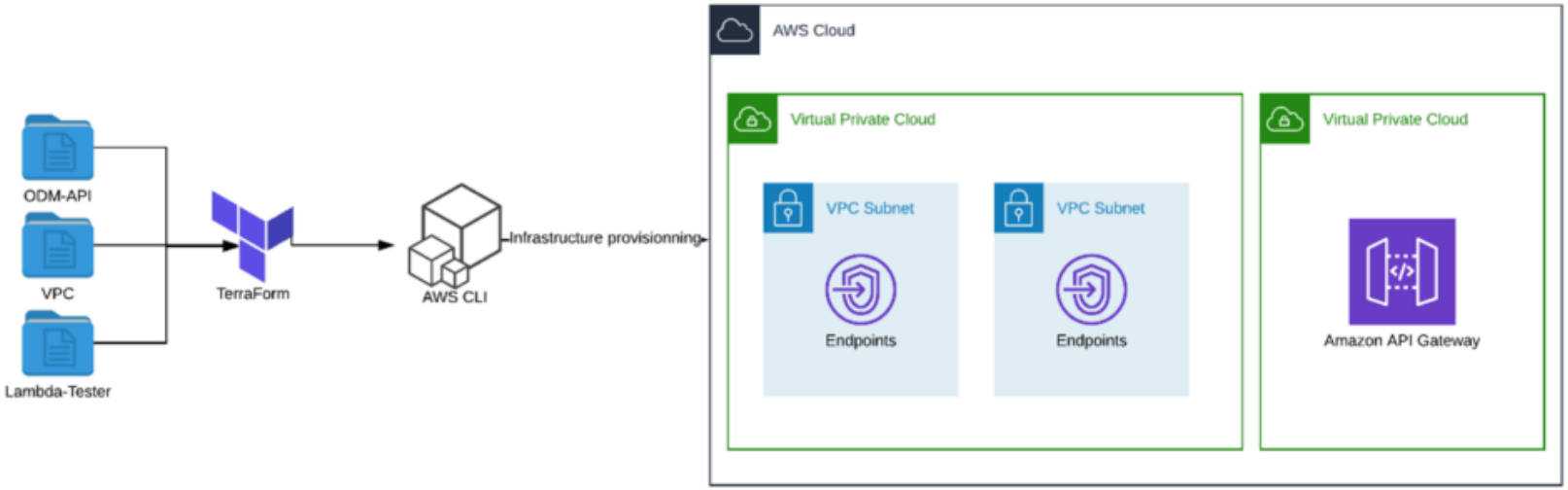
The developer can use Rule Designer as an Eclipse-based development environment of IBM Operational Decision Manager to create rule applications that automate the implementation of business policies. Once the rule application is created in the Rule Designer, the developer can migrate the application to a java standard edition environment to easily upload it to AWS Lambda which supports Java Runtimes (8,11).

Once the rule application is deployed to AWS Lambda, you can invoke it as a lambda function over HTTPS by defining a custom REST API and endpoint using Amazon API Gateway, and then mapping individual methods, such as GET and POST, to the specific Lambda function.

CloudLink case study: Software Business

Solution

Architecture - 2nd Phase



API Gateway private endpoints are made possible via AWS PrivateLink interface VPC endpoints. Interface endpoints work by creating elastic network interfaces in subnets that you define inside your VPC. Those network interfaces then provide access to the API Gateway running in its VPC.

CloudLink case study: Software Business

Benefits

API Gateway private endpoints enable use cases for building private API–based services inside your own VPCs. You can now keep both the frontend to your API (API Gateway) and the backend service (Lambda, EC2, ECS, etc.) private inside your VPC. Or you can have networks using Direct Connect networks without the need to expose them to the internet in any way. All of this without the need to manage the infrastructure that powers the API gateway itself!

Execution without servers is gaining traction. If you are unfamiliar with the definition, the idea is that you only supply the code you want to run, and the platform would magically make it available as a service. It is serverless, so you, the user, do not have to provide a server in any way, shape, or form. The best aspect, and the explanation for its recent success, is that you just pay for the execution time, while historically you will have to pay for the server to be up and running.

It is a very versatile and inexpensive approach of this type. In contrast to paying for provisioned idle servers that remain unused, the expense is dependent on what the organization needs. Serverless provides an unparalleled alignment between resource allocation and utilization of resources; a pair that is here with high-speed caching technologies and the next wave of elastic computing.