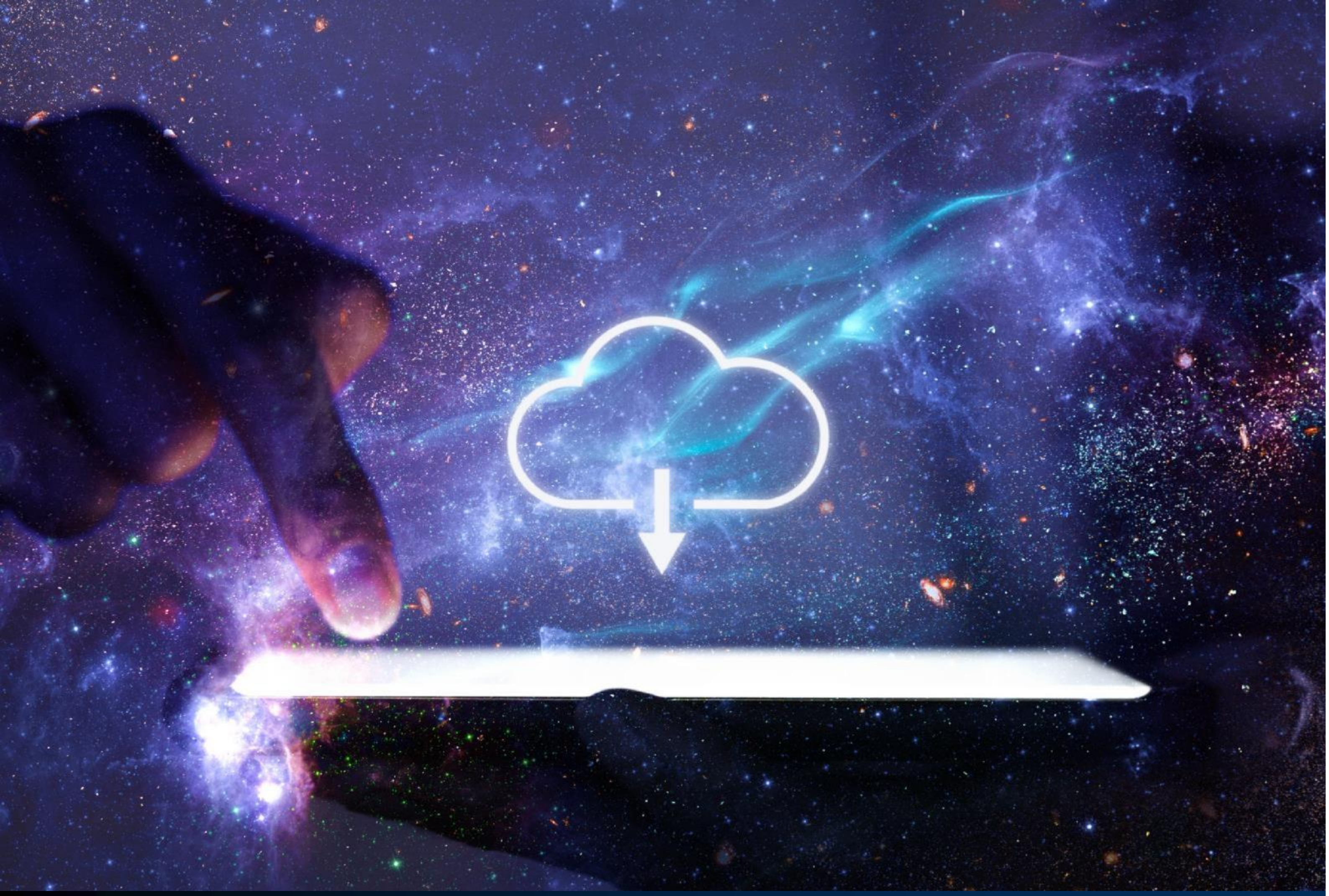


Amorphic Data Cloud

GxP Compliance Overview

Amorphic

Executive Summary

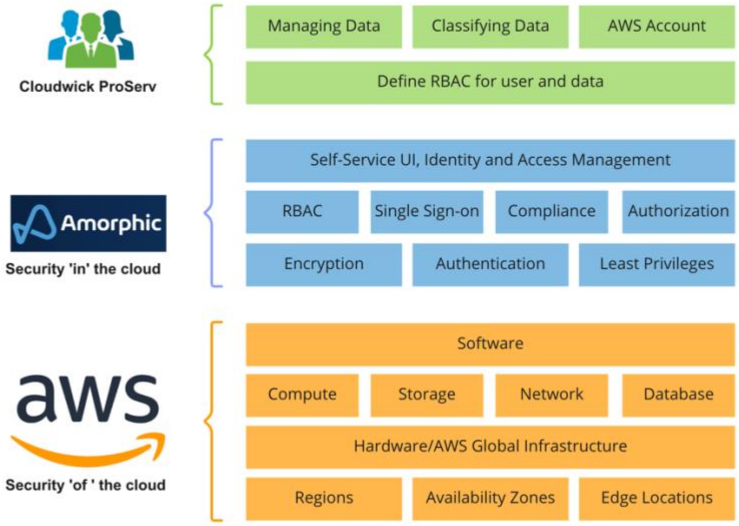
This whitepaper provides information on how Cloudwick approaches GxP-related compliance and security and provides customers guidance on using Amorphic Data Cloud in the context of GxP

What is shared responsibility model in Amorphic data cloud?

Amorphic data cloud is hosted on Amazon Web Services (AWS). Security and Compliance is a shared responsibility between AWS, Cloudwick and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages, and controls the components down to the physical security of the facilities in which the service operates.

Amorphic responsible for data encryption at rest and in motion. Amorphic follows AWS well architected framework when integrating different AWS services together by following the least privilege model. Amorphic is also responsible for managing authentication and authorization by configuring Identity and management in a secure way.

The Cloudwick professional services (in case of managed service) or customer assumes responsibility and management of providing access to the data and different analytical services within Amorphic data cloud



Amorphic Data Cloud shared responsibility model for GxP Compliance

AWS is responsible for the security and compliance of the Cloud, the infrastructure that runs all of the services offered in the AWS Cloud. Cloud security at AWS is the highest priority. AWS customers benefit from a data center and network architecture that are built to meet the requirements of the most security-sensitive organizations. infrastructure consists of the hardware, software, networking, and facilities that run AWS Cloud services.

21 CFR Part 11

Customers who use Amorphic Data Cloud to manage records in electronic form (e.g., those that are created, modified, maintained, archived, retrieved, or transmitted), under any records requirements set forth in agency regulations, are required to comply with applicable requirements within 21 CFR Part 11 Electronic Records; Electronic Signatures.

Part 11 was created to permit the adoption of new information technologies by FDA regulated life sciences organizations, while simultaneously providing a framework to ensure that the electronic GxP data is trustworthy and reliable.

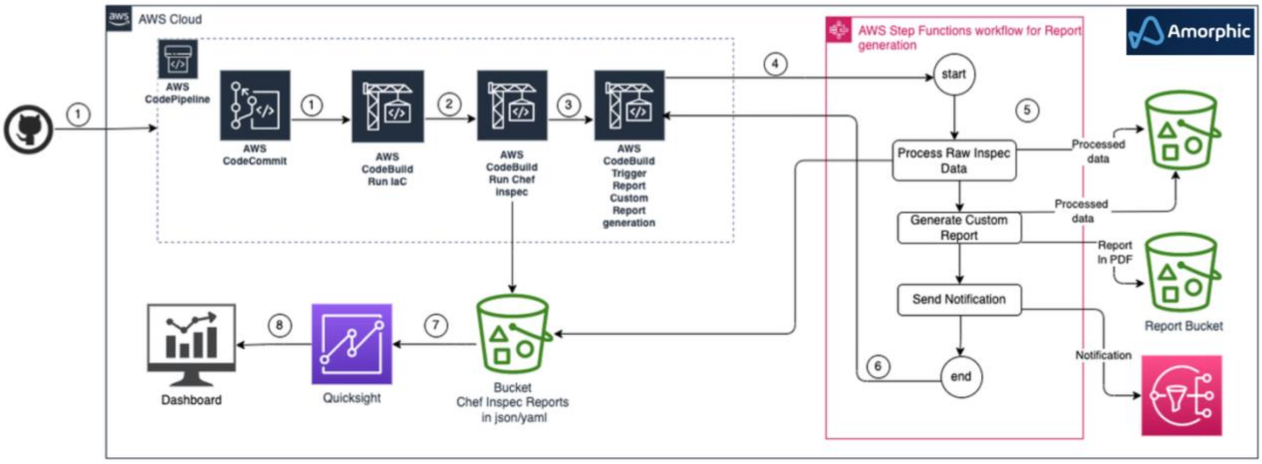
Amorphic Data Cloud has multiple functions that assist customers in demonstrating their compliance with 21 CFR Part 11 requirements, specifically around controls for closed systems and access control, audit logging, and records retention. Amorphic provides industry-leading features such as data encryption, MFA, key pair authentication and rotation, SSO, role-based access control, and more to ensure the highest levels of security for your account and users, as well as all the data you store in Amorphic.

Secure development processes

Every feature is implemented along with a permissions model for that feature in the Amorphic API. During the build and release processes Protego scans are run to ensure that secure coding processes are followed and that any dependencies do not have open vulnerabilities. Any high importance findings in those scans result in a build failure and are corrected. Cloudwick also uses ScoutSuite to do in-environment scans of the infrastructure which in turn feeds into upstream configuration as code.

GxP Infrastructure Installation Qualification on Amorphic Data Cloud

Amorphic automats the infrastructure Installation Qualification (IQ) steps of GxP Computer System Validation using Infrastructure as Code and Chef InSpec in the Amazon Web Services (AWS) environment. In GxP Computer System Validation, the underlying infrastructure supporting a regulated workload is required to be qualified to demonstrate controls for a closed system like Amorphic Data Cloud.



Amorphic Development (Infrastructure) Installation Qualification Process

Amorphic enables end-to-end automation of infrastructure Installation Qualification, from version control of script to protocol generation and dashboard for compliance monitoring.

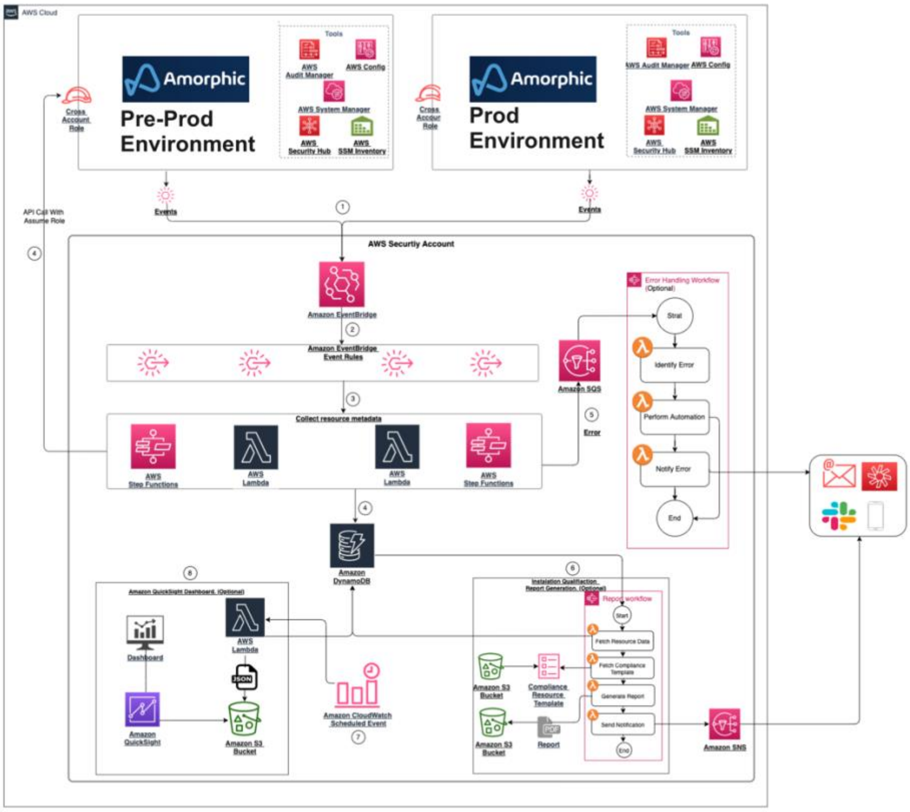
The following steps describes the automation workflow and highlights AWS services and processes for this automation. At the high level, there are three main categories of processes that triggers eight automated steps. The three categories are:

- CI/CD: BitBucket for version control, code build, infrastructure deployment, integration and tests (including InSpec).
- IQ: This is the post deployment steps. It runs the processes to validate resources and generate IQ protocol.
- Continuous Compliance: Monitors the resources' attributes for changes from the baseline. The dashboard displays deployed resources with alerts to resources that are different from expected.

Refer to the AWS blog to understand the eight automated steps for end-to-end Installation Qualification automation solution

GxP Continuous Compliance on Amorphic Data Cloud

The diagram below shows how Amorphic achieves continuous compliance reference architecture for GxP workloads.



Detailed architecture is explained in this blog

Automated Installation Qualification Report Generation in Amorphic

The automated Installation Qualification (IQ) process is a capability to create documents containing deployed AWS resources and verification test results that the infrastructure is configured as intended. The automated process allows you to run a list of tests and collect detailed attributes of deployed resources. It helps reduce overall time for the qualification process and provides accurate deployment attributes, which otherwise would need to be done manually.

Having an automated solution for infrastructure IQ improves consistency due to automation of development, deployment and testing processes. The following are some of the advantages of automating the IQ process:

- Cost reduction: Cost of managing infrastructure compliance can be reduced by decreasing manual efforts of updating documentation.
- Version control: The infrastructure environment can be governed by having the Infrastructure as Code script version controlled and roll back to the last good state upon failure.
- Repeatable: Infrastructure that you can replicate, re-deploy, and re-purpose. This solution can be centralized at a master account, organization unit or per app basis.

Amorphic automatically generates a PDF report. The report contains details of the deployed resources and verification results, comparing attributes of deployed resources against planned attributes. The comparison condition between expected value and actual value could be a range or a specific value depending on the test cases. The PDF report generation process can be setup to run as needed or upon any resource changes.

OWASP mitigations in Amorphic Data Cloud

The Open Web Application Security Project ® (OWASP) is a nonprofit foundation that works to improve the security of software. Periodically the foundation produces lists of the most common vulnerabilities found in Web Applications. Please request for more information about how Amorphic mitigated OWASP top ten vulnerabilities.

AWS services in Amorphic

Service Category	AWS Service	Purpose
Networking & Content Delivery	Amazon Route 53	Enables to provision, manage public domain names for Amorphic web portal and Morph.
	Amazon CloudFront	Securely deliver Amorphic web portal with low latency to end-user.
	Amazon Virtual Private Cloud	To logically isolate and secure AWS resources.
	Internet Gateway	Enable resources in a public subnet to connect to the internet or other AWS services and allows end-user to initiate connections from the internet to internetfacing resources.
	NAT Gateway	Enable Squid proxy server in a private subnet to connect to the Internet.
	NAT Gateway EIP	Elastic IP address to associate with the NAT gateway.
	Virtual Private Gateway	Enable to terminate VPN connections from on-prem or customer environments.
	Transit Gateway	Enable to terminate VPN connections, Direct Connections from on-prem or customer environments and peer with other VPCs.
	Transit Gateway ENI	Enables to attach a Transit Gateway with VPC.
	Customer Gateway	Provides on-prem or customer environments Customer Gateway Device information to AWS.
	Subnet Route Tables	Route north-south and east-west VPC traffic.
	Subnet Network ACLs	Control traffic in and out of subnets.
	Security Groups	Control traffic in and out of network interfaces.

	SageMaker API Interface Endpoint	Securely connect to SageMaker API regional endpoint within the AWS network.
	SageMaker Notebook Interface Endpoint	Securely connect to SageMaker Notebook regional endpoint within the AWS network.
	S3 Gateway Endpoint	Securely connect to S3 regional endpoint within the AWS network.
	DynamoDB Gateway Endpoint	Securely connect to DynamoDB regional endpoint within the AWS network.
	Amazon Glue Public Connection	Elastic Network Interface to pull data from public JDBC data sources.
	Amazon Glue Private Connection	Elastic Network Interface to pull data from private JDBC data sources via AWS Direct Connect or VPC Peering.
	Flow Logs	Capture information about the IP traffic going to and from network interfaces.
	Application Load Balancer	External Application Load Balancer distributes incoming traffic from end-user to Morph web service hosted in EC2 instances.
	Network Load Balancer	External Network Load Balancer distributes incoming traffic from end-user to Redshift.
	AWS Site-to-Site VPN	Enable secure IPsec tunnel between on-prem or customer environments and VPC.
	AWS Direct Connect	Enable secure private connectivity between on-prem or customer environments and VPC.
Data Warehouse	Amazon Aurora MySQL	Data warehouse to securely stores and manage datasets.
	Amazon Redshift	Data warehouse to securely stores and manage datasets.
Database	Amazon DynamoDB	Non-relational database to securely store metadata of dataset and user access permissions.

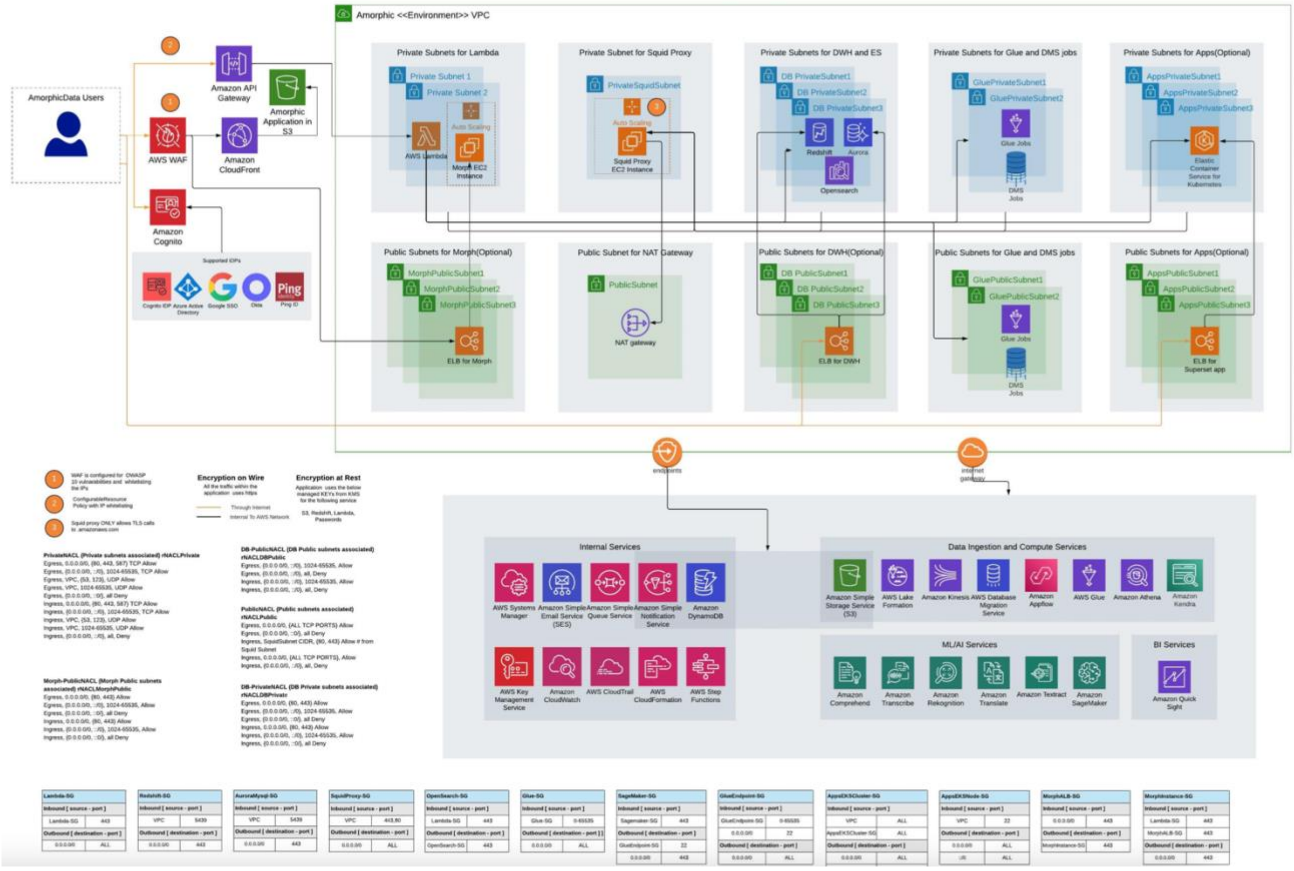
Storage	Amazon S3 bucket	Securely store static contents of Amorphic web portal
	Amazon S3 bucket	Securely store data uploaded by users.
	Amazon Elastic Block Store	Block-storage for Morph and Squid servers.
Compute	AWS Lambda	Run the Amorphic serverless backend service in response to API calls via Amazon API Gateway.
	AWS Lambda@Edge	Run Lambda functions to customize CloudFront content delivery.
	AWS EC2	EC2 instance to host Morph.
	AWS EC2	EC2 instance to host Squid proxy.
Application Integration	AWS Step Functions	Orchestrate the AWS account preparation and application deployment process.
	Amazon Simple Notification Service	Enables configuring event triggers for backend AWS Lambda functions.
	Amazon Simple Queue Service	Enables to process AWS Lambda Dead Letter Queues.
	Amazon API Gateway	Securely process API calls from end-users and facilitate API management.
Analytics	Amazon Athena	Enable end-user to query on data or datasets stored in Amazon S3 buckets.
	Amazon Elasticsearch Service	Provide fast text search capability for end-users on datasets.
	Amazon Kinesis	Stream data into Amorphic Data platform using Amazon Kinesis Firehose.
	Amazon QuickSight	Enable end-user to create and publish interactive BI dashboards.
	Amazon Glue	Enable end-user to run ELT jobs.
Machine Learning	Amazon SageMaker	Enable end-user to run ML models.

	Amazon Comprehend	Enables end-user to leverage NLP to find insights and relationships from datasets.
	Amazon Translate	Implements neural machine translation service in enduser ML models.

	Amazon Textract	Enables end-user to extracts structured and unstructured data from document datasets.
	Amazon Transcribe	Enable end-user to apply Speech to Text capability on ML datasets.
	Amazon Rekognition	Enable end-user to analyse video and image datasets.
Migration & Transfer	AWS Database Migration Service	Ingest or replicate data from databases sources to the Amorphic data lake.
Security, Identity & Compliance	AWS Identity & Access Management (IAM)	Provide role-based access control to AWS services and resources.
	Amazon Cognito	Authenticate and authorise users and API calls, enable social and enterprise identity federation.
	AWS CloudTrail	Store audit logs generated by AWS for end-user access and API calls to the Amorphic for security and compliance purpose.
	Amazon GuardDuty	Enables continuously monitors for malicious activity and unauthorized behaviour in AWS accounts.
	Amazon Macie	Enables to discover and protect data store in Amazon S3 buckets using machine learning and pattern matching.
	AWS Web Application Firewall	Implement guardrails based on IP whitelists and access controls to mitigate OWASP top 10 vulnerabilities.

	AWS Key Management Service	Generate and manage encryptions keys used to encrypt data stored in Amazon S3 buckets, Amazon Redshift, Amazon Elasticsearch Service, Amazon RDS Aurora, Amazon Glue, Amazon Lambda, AWS Systems Manager, AWS Certificate Manager, and AWS Secrets Manager.
	AWS Certificate Manager	Enables to provision, manage public SSL certificate for Amorphic web portal and Morph.
Management & Governance	Amazon CloudWatch	Monitor the AWS services and stores logs generated by AWS services and Amorphic Data.
	AWS CloudFormation	Enables Infrastructure as Code for Amorphic components and supports infrastructure versioning.
	AWS Systems Manager Parameter Store	Enables secure storage and management environment variables, CloudFormation parameters and outputs.
	Amazon Simple Email Service	Send email alerts and send end-user verification emails.
	AWS Cost Explorer	Enable customer to manage AWS costs and usage.
	AWS Config	Enable configuration drift monitoring.

Amorphic security architecture



1 WAF is configured for OWASP 10 vulnerabilities and whitelisting the IPs

2 ConfigurableResource Policy with IP whitelisting

3 Squid proxy ONLY allows TLS calls to .amazonaws.com

Encryption on Wire

All the traffic within the application uses https

Encryption at Rest

Application uses the below managed KEYs from KMS for the following service

S3, Redshift, Lambda, Passwords

PrivateNACL (Private subnets associated) rNACLPrivate
Egress, 0.0.0.0/0, (80, 443, 587) TCP Allow
Egress, (0.0.0.0/0, ::/0), 1024-65535, TCP Allow
Egress, VPC, (53, 123), UDP Allow
Egress, VPC, 1024-65535, UDP Allow
Egress, (0.0.0.0/0, ::0/), all Deny
Ingress, 0.0.0.0/0, (80, 443, 587) TCP Allow
Ingress, (0.0.0.0/0, ::/0), 1024-65535, TCP Allow
Ingress, VPC, (53, 123), UDP Allow
Ingress, VPC, 1024-65535, UDP Allow
Ingress, (0.0.0.0/0, ::/0), all, Deny

Morph-PublicNACL (Morph Public subnets associated) rNACLMorphPublic
Egress, 0.0.0.0/0, (80, 443) Allow
Egress, (0.0.0.0/0, ::/0), 1024-65535, Allow
Egress, (0.0.0.0/0, ::0/), all Deny
Ingress, 0.0.0.0/0, (80, 443) Allow
Ingress, (0.0.0.0/0, ::/0), 1024-65535, Allow
Ingress, (0.0.0.0/0, ::0/), all Deny

DB-PublicNACL (DB Public subnets associated) rNACLDBPublic
Egress, (0.0.0.0/0, ::/0), 1024-65535, Allow
Egress, (0.0.0.0/0, ::/0), all, Deny
Ingress, (0.0.0.0/0, ::/0), 1024-65535, Allow
Ingress, (0.0.0.0/0, ::/0), all, Deny

PublicNACL (Public subnets associated) rNACLPublic
Egress, 0.0.0.0/0, {ALL TCP PORTS} Allow
Egress, (0.0.0.0/0, ::0/), all Deny
Ingress, SquidSubnet CIDR, (80, 443) Allow # from Squid Subnet
Ingress, 0.0.0.0/0, {ALL TCP PORTS}, Allow
Ingress, (0.0.0.0/0, ::/0), all, Deny

DB-PrivateNACL (DB Private subnets associated) rNACLDBPrivate
Egress, 0.0.0.0/0, (80, 443) Allow
Egress, (0.0.0.0/0, ::/0), 1024-65535, Allow
Egress, (0.0.0.0/0, ::0/), all Deny
Ingress, 0.0.0.0/0, (80, 443) Allow
Ingress, (0.0.0.0/0, ::/0), 1024-65535, Allow
Ingress, (0.0.0.0/0, ::0/), all Deny

Lambda-SG	
Inbound [source - port]	
Lambda-SG	443
Outbound [destination - port]	
0.0.0.0/0	ALL

Redshift-SG	
Inbound [source - port]	
VPC	5439
Outbound [destination - port]	
0.0.0.0/0	443

AuroraMysql-SG	
Inbound [source - port]	
VPC	5439
Outbound [destination - port]	
0.0.0.0/0	443

SquidProxy-SG	
Inbound [source - port]	
VPC	443,80
Outbound [destination - port]	
0.0.0.0/0	ALL

OpenSearch-SG	
Inbound [source - port]	
Lambda-SG	443
Outbound [destination - port]	
OpenSearch-SG	443

Glue-SG	
Inbound [source - port]	
Glue-SG	0-65535
Outbound [destination - port]]	
0.0.0.0/0	ALL

SageMaker-SG	
Inbound [source - port]	
Sagemaker-SG	443
Outbound [destination - port]	
GlueEndpoint-SG	22
0.0.0.0/0	443

GlueEndpoint-SG	
Inbound [source - port]	
GlueEndpoint-SG	0-65535
0.0.0.0/0	22
Outbound [destination - port]	
0.0.0.0/0	ALL

AppsEKSCluster-SG	
Inbound [source - port]	
VPC	ALL
AppsEKSCluster-SG	ALL
Outbound [destination - port]	
0.0.0.0/0	ALL

AppsEKSNode-SG	
Inbound [source - port]	
VPC	22
Outbound [destination - port]	
0.0.0.0/0	ALL
::/0	ALL

MorphALB-SG	
Inbound [source - port]	
0.0.0.0/0	443
Outbound [destination - port]	
MorphInstance-SG	443

MorphInstance-SG	
Inbound [source - port]	
Lambda-SG	443
MorphALB-SG	443
Outbound [destination - port]	
0.0.0.0/0	443

References

GxP systems on AWS

Automating GxP Infrastructure Installation Qualification on AWS with Chef InSpec

GxP Continuous Compliance on AWS

About Amorphic Data Cloud

Amorphic Data Cloud is a fully managed self-service data lake platform that simplifies AWS analytics for IT and non-IT users. The platform is offered as both a Software-as-a-Service and a managed subscription for AWS that automates, orchestrates and simplifies AI services, Machine Learning, and Analytics for engineering, business and data science teams. It extends and enhances the power of cloud data warehouse and business intelligence for all data and users by providing one unified analytics platform to Ingest, Analyse, and Visualize data natively.

About Cloudwick

Cloudwick is an AWS certified Advanced Consulting Partner that specializes in building native data lakes that power faster, cheaper, and more agile cloud analytics for IT, business users, and data scientists. Whether you need to migrate your analytics to the cloud, add decision automation to your business intelligence, improve customer experience with machine learning or want to build or buy a data lake, Cloudwick has a complete portfolio of services and solutions.

December 2022

CONTACT US:

Corporate Office

39899 Balentine Drive,
Suite 345 – 350
Newark, CA 94560

India Office

Cloudwick Technologies India Pvt.
Limited, c/o WeWork - B101, 8th
floor, RMZ Latitude Commercial,
Bellary Rd., Hebbal,Bengaluru,
Karnataka 560024 India

UK Office

Suite 101, Devonshire House,
29 - 31 Elmfield Road, Bromley
BR1 1LT, London

Website: www.amorphicdata.com
Email: sales@amorphicdata.com

Amorphic