Architectural Design and Overview of Proposed Healthcare Application

- Group 26

Table of Contents

Executive Summary

The document details a comprehensive upgrade of a healthcare application's architecture using Amazon Web Services (AWS). It outlines existing infrastructure, including web, application, and database servers, and highlights the need for enhanced security protocols. Key changes proposed include improved Identity and Access Management (IAM), multi-region deployment for disaster recovery, and stronger data encryption. The summary emphasizes the adoption of AWS services for monitoring, compliance, and data management to ensure a secure, efficient, and compliant environment for healthcare applications.

Existing Infrastructure

The healthcare company's application infrastructure is structured around distinct components, contains web servers dedicated to frontend services and user interaction, application servers responsible for processing business logic, and database servers that store critical data such as product information, user details, and medical histories. Operating within Amazon Web Services (AWS), this infrastructure relies on the utilization of virtual machines (VMs) to host healthcare applications and databases.

The network architecture is designed with various virtual networks and subnets tailored for different departments, all managed and regulated through Identity and Access Management (IAM) to govern user access to resources. The IT department holds complete access to both frontend and backend instances for administrative purposes, with IP addresses being automatically assigned. To ensure scalability, the Virtual Private Cloud (VPC) has been designed to accommodate potential growth and increased demand. Access to the web servers involves DNS routing, enabling efficient communication between users and the frontend services.

Presently, there is an absence of comprehensive web application security protocols, potentially leaving the system vulnerable to various cyber threats and attacks. Additionally, the absence of encryption of various resources and several other missing critical security features exposes the infrastructure to significant vulnerabilities.

It is critical to address the absence of web application security measures and the lack of backup encryption within the infrastructure. Implementing robust security protocols, including encryption for backups, firewalls, intrusion detection systems, regular security audits, and other essential security features, is imperative. These measures not only protect the system against potential security threats but also protect sensitive healthcare data and ensure compliance with industry regulations.

Infrastructure Changes

Identity and Access Management (IAM)

- **IAM roles assigned for IT personnel:**
  Role-based access control (RBAC) in IAM has been implemented to create and manage permissions for various IT personnels based on their functional responsibilities and roles they play in the system. We make sure that every role has the exact set of permissions needed to carry out its assigned duties by giving IAM roles to users or groups.

  Following are the permissions attached to different IT Personnels.

IT Personnel Role	IAM Permissions Assigned
End User Support	AmazonWorkSpacesReadOnly AmazonConnectReadOnly AmazonEC2ReadOnlyAccess AWSHealthReadOnlyAccess IAMReadOnlyAccess
DB Admins	AmazonRDSFullAccess AmazonDynamoDBFullAccess AWSKeyManagementServicePowerUser CloudWatchReadOnlyAccess AmazonRedshiftReadOnlyAccess
Data Engineer	AmazonRDSFullAccess AmazonDynamoDBFullAccess AmazonRedshiftFullAccess AWSGlueFullAccess AmazonS3FullAccess
Network Admins	AmazonVPCFullAccess AWSCloudTrailReadOnlyAccess AWSDirectConnectReadOnlyAccess ElasticLoadBalancingReadOnlyAccess AWSNetworkManagerReadOnlyAccess
System Admin	AmazonEC2FullAccess AmazonS3FullAccess AWSLambdaFullAccess CloudWatchFullAccess AWSConfigRulesExecutionRole
Super Admin	AdministratorAccess

	AWSKeyManagementServiceFullAccess AWSConfigFullAccess AWSHealthFullAccess CloudWatchFullAccess
Application Developer	AWSLambdaFullAccess AmazonEC2FullAccess AmazonS3FullAccess AWSCodeDeployFullAccess CloudWatchFullAccess
Third-party IT Support Consultants	AWSReadOnlyAccess AmazonEC2ReadOnlyAccess AmazonS3ReadOnlyAccess CloudWatchLogsReadOnlyAccess IAMReadOnlyAccess

- **Enforced Multi-Factor Authentication (MFA):**
  Multi-Factor Authentication (MFA) has been enforced as a compulsory measure for system access. This enhanced security protocol requires users to furnish more than one proof of identity.

Regions:

The existing infrastructure is currently located within a single region, which poses potential risks of compromising data and making it unavailable for patients and care providers. To mitigate these risks and ensure continuity of operations, we've implemented a multi-region involving the utilization of an additional region by replicating the infrastructure.

This method assures redundancy and continuity of operations, addressing issues such as data compromise and unavailability. The secondary location was chosen based on several factors, such as service availability, redundancy, compliance needs, and geographic closeness to improve the infrastructure's resilience and efficiency for both patients and healthcare professionals.

Primary Region: us-east-1

Secondary/ DR region: us-west-1

We configured these regions to be in Active-Passive mode by performing full back up on weekly basis and an incremental backup in the off-hours.

Enhancing Encryption and Data Protection:

- **Amazon EBS encryption**
  In the existing infrastructure the data at rest and data at transit is not protected, We Used Amazon EBS encryption to encrypt data at rest.
  When it comes to sensitive or regulated data, we have used key pairs to encrypt traffic coming to and from the EC2 instances, we also made sure that Access to EC2 instances is limited to individuals who have the corresponding private key by utilizing key pairs. By using a strong authentication system, this improves security by reducing the possibility of unauthorized access and communication eavesdropping.

- **Amazon S3 encryption:**
  By encrypting data as it moves across the network, Amazon S3 encryption adds a crucial layer of security, protecting it from possible interception or unauthorized access while in transit. Because of its transparency, we easily incorporate encryption into data transfer procedures without having to worry about making specific coding adjustments.

- **AWS Key Management Service (KMS):**
  The fully managed encryption service AWS Key Management Service (KMS) gives the ability to generate, administer, and control the cryptographic keys needed to encrypt and decrypt any type of cloud data. While CloudTrail automatically encrypts all log data, we use AWS KMS to encrypt log files while they are at rest. This gives the log data an extra degree of security.

- **Encrypting RDS instances:**
  To protect sensitive data inside a database, we enable Relational Database Service (RDS) encryption. Data at rest is safeguarded by using encryption, which stops unwanted access to the database files.

Organization Network: (Enhancing Network and Network Security)

- **Route53:**
  We have used Route53 for our health care web application to be accessible over the internet to end users. As patients, care providers and IP employees are required to access MedCircle application over internet it helps in resolving our domain to an IP address and route internet traffic to the AWS resource based on resource record sets we created.

- **NAT Gateway**: We used NAT gateway to prevent direct inbound internet traffic to access our EC2 instances. It also facilitates outbound internet traffic from our internal network and AWS resources which is needed for software updates, security patches, backup and recovery as the resources in private subnets are not allowed to reach internet directly.

- **Internet Gateway**: It acts as a doorway between the AWS network and the internet, enabling bi-directional communication between AWS resources and the internet. Only resources in a public subnet can access the internet and anyone can connect to this resource back from internet using its public IP with security group of resource strictly applied.
  In our infrastructure now, we included an internet gateway as IT employees must access EC2 instances on regular basis and patients must access their test results, upload documents into backend storage containers like RDS/ S3.

- **AWS Client VPN:** As our IT employes working from home need to have access to the resources in our AWS cloud a secure point-to-point connection from remote users to the AWS network is required. We used AWS Client VPN which allows access to resources as if they were on a local network.

- **PaloAlto External Firewall:**
  We used PaloAlto next generation firewall as our external firewall, which offers advanced network security features, such as Advanced Threat Prevention, Traffic Visibility and Control, Intrusion Prevention System (IPS), Application Control, URL Filtering, Threat Intelligence Integration, Sandboxing, User Identification and Control, VPN Support, High Availability and Scalability etc. to protect the network from unauthorized access and other cyber threats.
  We have configured our Pal Alto Networks' firewalls in an active/passive high availability (HA) setup to ensure continuous network protection, uptime and availability.

- **Elastic Load Balancer:**
  We have used an application load balancer that Automatically distributes incoming application traffic across multiple EC2 instances, ensuring high availability and fault tolerance in our applications.

- **AWS Site-to-Site VPN:** Our IT employees and Care providers working from on-premise network securely need to connect to AWS VPC. AWS S2S VPN helps in achieving that through an encrypted channel.

- **Checkpoint Internal Firewalls:** We have used checkpoint firewalls as our internal firewalls which provides robust security architecture defending the network from intrusions, malware, and other cyber threats while facilitating secure data transfer and communication within the network.
  We have configured our internal firewalls in a active standby mode.
- **NACL**
  For subnet traffic control, we used Network Access Control Lists (NACLs). These stateless firewalls are used to allow or block specific IP addresses because they allow and deny traffic based on IP address/subnet and network port.

- **Security groups:**
  For better control over traffic between AWS VPC resources, we used multiple Security Groups. We use a security group, for instance, for web-based services that permits database traffic to exit and HTTP / HTTPS traffic to enter, and a database security group that permits database traffic to enter from the web servers' group. Once more, this adheres to the "least privilege" principle, which states that resources can only communicate with one another through the necessary ports.
  In the existing infrastructure setup, there was an oversight where the access controls for EC2 and RDS instances were not properly restricted, leaving these resources exposed and susceptible to potential vulnerabilities.

For EC2 Instances:

	Source	Destination	Port(s)
Inbound Rule	Private VPN	Private AS	ssh
	Private LB	Private WS	http
Outbound Rule	Private AS	Private RDS	TCP-3306

For RDS Instances:

	Source	Destination	Port(s)
Inbound Rule	Private AS Private VPN	Private RDS	TCP-3306
Outbound Rule	Private RDS	Private NAT GW	TCP/Custom Port

Web Application Security:

The current infrastructure has no protection against web-based attacks we have involved various elements such as IAM MFA Token, AWS Client VPN, AWS Sheild, Barracuda WAFs, Palo Alto Firewalls, Elastic Load Balancers, and AWS identity and monitoring services. Barracuda WAF (Web Application Firewall plays a crucial role in this setup.

Key features of Barracuda WAF as an external WAF include protection against Web-Based Threats, Automated Vulnerability Remediation, DDoS Protection, SSL Offloading, Access Control, Data Loss Prevention and it enhances application performance.

Network Segmentation:

Region	Zone	Service	Subnet (IP Range)
Primary	Availability Zone 1	Private Application Server (AS)	10.0.0.0/24
		Private Workstation (WS)	10.0.1.0/24
		Private Relational Database Service (RDS)	10.0.10.0/24
		External PaloAlto Firewalls (FW)	10.0.20.0/28
		Barracuda Web Application Firewall (WAF)	10.0.20.20/28
		Application Load Balancer (LB)	10.0.20.16/28
		Public Internet Gateway (IGW)	10.0.20.32/28
		Private Internet Gateway (IGW)	10.0.20.48/28
		Public NAT Gateway	10.0.20.64/28
		Private NAT Gateway	10.0.20.96/28
		Private VPN	10.0.20.112/28
		Out of Band subnet:	10.0.20.128/28
	Availability Zone 2	Private Application Server (AS)	10.0.30.0/24
		Private Workstation (WS)	10.0.31.0/24
		Private Relational Database Servers (RDS)	10.0.32.0/24
Secondary	Availability Zone 1	Private Application Server (AS)	10.1.0.0/24
		Private Workstation (WS)	10.1.1.0/24
		Private Relational Database Service (RDS)	10.1.10.0/24
		External PaloAlto Firewalls (FW)	10.1.20.0/28
		Barracuda Web Application Firewall (WAF)	10.1.20.16/28
		Application Load Balancer (LB)	10.1.20.32/28
		Public Internet Gateway (IGW)	10.1.20.48/28
		Private Internet Gateway (IGW)	10.1.20.64/28
		Public NAT Gateway	10.1.20.80/28
		Private NAT Gateway	10.1.20.96/28
		Private VPN	10.1.20.112/28
		Out of Band subnet	10.1.20.128/28
	Availability Zone 2	Private Application Server (AS)	10.1.30.0/24
		Private Workstation (WS)	10.1.31.0/24
		Private Relational Database Servers (RDS)	10.1.32.0/24

Compute and Data Storage

- **EC2**

  An EC2 instance serves as a pivotal virtual server within the AWS cloud, offering scalable computing capabilities tailored to diverse workloads. We have evaluated and refined the existing EC2 instance configuration, implementing several key enhancements and adjustments.

  We have made below modifications to the EC2 instance setup:

Feature	Description
Instance Type Upgrade	Upgraded to the R5 instance type, which optimized the system for high-capacity performance and increased effectiveness in managing a range of workloads
Kernel Version Update	Ensured that the most recent kernel version was installed to improve system security, reliability, and compatibility with the newest AWS features and services.
Robust Patch Management	To guarantee prompt deployment of security updates and improvements, the AWS Systems Manager (SSM) Patch Manager was utilized to centrally and efficiently manage patch updates.
Fine Grained Access Control	Strengthens overall security by giving authorized entities specific and restricted access levels to the EC2 instance through the assignment of relevant IAM roles.
AMI Handling and Backups	For quick instance recovery and configuration replication, an S3 repository in the us-west-1 region is used to create and maintain an up-to-date Amazon Machine Image (AMI).
Auto Scaling for Elasticity	Enabled Auto Scaling features to dynamically alter instance capacity based on workload demands, guaranteeing effective resource usage and responsiveness.
EnhancedSecurity Measures	To reduce vulnerability to outsider attacks, more security layers were put in place, such as deletion protection, frequent snapshot backups, and public IP assignment disabling.
EnhancedMetadata Security	To strengthen instance metadata security and thwart possible exploitation, Instance Metadata Service Version 2 (IMDSv2) was activated.
Comprehensive Monitoring	Enabled extensive monitoring for resource optimization, actionable insights into system activity, and thorough instance performance tracking by employing features like CloudWatch and CloudTrail.

Instance Profile: We have enforced different IAM Roles to handle security credentials for safe API requests from EC2 instances. To make sure the role only has the rights required for the application, we utilized IAM Access Analyzer to develop a policy for the IAM role based on observed access behaviors.

Automatic Scaling Group (ASG): We use ASG to proactively modify the instance count prior to resource depletion to guarantee continuous availability of EC2 instances. Elastic Load Balancing (ELB) and ASG work well together, making resource increase easier.

EC2 Backup and Recovery: To create a repeatable configuration for starting new instances or replacing faulty ones, we used Amazon Machine Images (AMI) for thorough backups. Furthermore, backup volumes can be created by taking a picture of each individual volume connected to an EC2 instance. If data is corrupted or fails, these backups are essential for replacing volumes.
We have also exported the Elastic Block Store (EBS) volume to a separate region for cross region backup, making sure the snapshots are encrypted in accordance with compliance requirements.

- **EBS**

  Because of its reliable, low-latency performance, EBS is a crucial component of our infrastructure, serving as scalable and sturdy block storage for our EC2 instances. It is also essential for database-intensive applications due to their consistent, low-latency performance.

Feature	**Description**
Encryption	When connecting EBS to an EC2 instance, this functionality, which uses AWS Key Management Service (KMS) for volume encryption, is enabled.
Fast Snapshot	In an emergency, this option is turned on to recover volume more quickly.
Snapshot management	Subsequent snapshots only capture incremental block-level changes; initial snapshots are entire volume copies. By default, AWS-managed keys are used for encryption on EBS volumes and snapshots.

- **RDS**

  RDS is essential to our infrastructure's handling of private patient information. Strong data security and recovery capabilities are ensured by the configuration. Scheduled regular backups are made to prevent data loss and to aid in disaster recovery.

Additionally, this configuration offers fallback alternatives and point-in-time recovery in case of any problems during system upgrades. An important priority is adhering to regulatory requirements and policies. The database is encrypted using the industry standard AES-256 encryption technique, which boosts security by guaranteeing that all logs, backups, snapshots, and stored data are safely encrypted. This all-encompassing strategy guarantees a database environment that is safe, dependable, and compliant.

Feature	**Description**
Credentials	There are stringent standards for the length and complexity of usernames and passwords.
Deletion Protection	Activated to safeguard data.
Backups & Snapshots	S3 buckets are used for automated daily backups, cross-region replication, and manual database snapshot capabilities.
Retention Period	The 35-day retention period has been set.
Encryption	Default encryption for data security.
ASG & Monitoring	Autoscaling and monitoring tools are integrated with ASG.
High Availability	Achieved By using read replicas and multi-AZ deployments.
PerformanceMonitoring & Security	Performance Insights, Security Groups, and VPC integration are used in performance monitoring and security.
Scalability and Automatic Updates	This section covers storage autoscaling and software patching.
Alerts	Social network notifications of database events.

- **S3Bucket:**

  S3 in our infrastructure is a central component for data storage, security, processing, and integrated with various AWS services to enhance its capabilities.

Feature	**Description**
S3 Object Lambda Access Points	Allows AWS Lambda functions to be executed directly within S3 for data transformation and processing operations.

Data Storage Group with Amazon Macie	Integrated for improved privacy and data security, machine learning is used in S3 to find, identify, and safeguard sensitive data.
Data Encryption Key Management	Used data encryption keys to protect encrypted data that is in the background.
Amazon S3 Snapshot Backup	Offers a mechanism for generating data backups and snapshots for durability and restoration.
Bucket Versioning	Multiple versions of an object can be kept in the same bucket, which is helpful for recovering from inadvertent overwrites or deletes.
Object Lock	Activated to stop objects from being replaced or erased for a predetermined period or forever.
MFA Delete	Activated to delete objects, multi-factor authentication is needed. This provides an extra degree of protection against inadvertent or deliberate removals.
Replication Rules	Configured to automatically duplicate objects between S3 buckets for redundancy inside or between regions, improving disaster recovery and data availability.
SSE-KMS encryption	Enabled for more protection and control over the encryption keys, utilize Server-Side Encryption with AWS Key Management Service (KMS).
Server Access Logging	Enabled to trace requests sent to the S3 bucket, which is important for compliance and security audits.

Services and Methodologies

1. IAM & MFA Token

Usage: Identity and access management, including multi-factor authentication for enhanced security.
Vulnerability Mitigation: Addresses the lack of MFA, ensuring that users with administrative access are securely authenticated.

2. AWS Client VPN

Usage: Secure connection for remote users to AWS resources.
Vulnerability Mitigation: Provides secure network access, mitigating risks related to network segmentation and firewall configurations.

3. Prod VPC & DMZ Subnet

Usage: Network isolation and segmentation.
Vulnerability Mitigation: Addresses poor network segmentation and weak security group configuration, reducing the attack surface.

4. AWS Cloud & US East-1 Region

Usage: Cloud infrastructure services distributed across multiple regions.
Vulnerability Mitigation: Enhances disaster recovery and regional resilience.

5. AWS Identity Services (Amazon Cognito, Directory Service)

Usage: User authentication and directory services.
Vulnerability Mitigation: Strengthens access controls and identity management.

Amazon Cognito

Amazon Cognito in AWS is a fully managed service designed to handle user identity and access management for web and mobile applications. It facilitates user authentication through various methods, including username/password and social identity providers. Cognito manages user directories, offering features such as user registration, account recovery, and verification. The service supports identity federation, enabling users to sign in with credentials from external providers. With seamless integration into AWS Identity and Access Management (IAM), Cognito ensures secure and fine-grained access control to AWS resources, making it a comprehensive solution for developers to handle user authentication and authorization in their applications.

Directory Services

AWS Directory Service is a managed service that simplifies the deployment and management of directories for identity and access management. It allows organizations to connect their AWS resources to existing on-premises Microsoft Active Directory or to create a new, fully managed directory in the AWS Cloud. AWS Directory Service supports multiple directory types, including Simple AD, AD Connector, and Microsoft AD, offering flexibility based on specific use cases. It enables seamless and secure integration between AWS workloads and on-premises environments, providing a unified identity solution. Additionally, AWS Directory Service enhances security by allowing administrators to enforce access controls and policies across AWS resources.

6. AWS KMS & Data Encryption Key

Usage: Key management service for data encryption.
Vulnerability Mitigation: Mitigates risks related to data encryption, addressing vulnerabilities in RDS, EC2, and S3.

AWS KMS
AWS Key Management Service (KMS) is a managed service that enables the creation and control of encryption keys for securing sensitive data. It simplifies the process of managing cryptographic keys used to encrypt data across various AWS services and in custom applications. KMS provides a secure and scalable key storage solution, ensuring the protection of keys with hardware security modules (HSMs). It supports the creation of customer master keys (CMKs) and allows users to define access policies, granting specific permissions for key usage. With integration into various AWS services, AWS KMS ensures the encryption and decryption of data at rest and in transit, offering a robust and centralized key management solution.

7. AWS Monitoring Services (CloudWatch, Trusted Advisor, AWS Config)

Usage: Monitoring and advising on AWS resource configurations.
Vulnerability Mitigation: Enables detection and alerts for security issues, such as misconfigurations and compliance violations.

CloudWatch
CloudWatch is a real-time log monitoring tool which also proactively monitors the performance metrics of AWS resources that are associated with it, helps in troubleshooting based on the alerts and ensures timely response to any security incidents or can trigger automated actions based on alarm set.

In our infrastructure, we associated CloudWatch with many other services like EC2 instances, RDS DB, S3 bucket, Elastic Load Balancer (ELB), DynamoDB, Lambda functions, API gateway.

AWS Config
Having this service enabled helps us to record configuration changes of all AWS resources in our AWS account and notifies the owner. This enables compliance checks against industry standards and stays compliant.AWS config is integrated with other services like CloudWatch for logging, Lambda function for automated responses, SNS (Simple Notification Service) for sending notification to owner.

AWS Trusted Advisor

AWS Trusted Advisor is a service that provides real-time guidance to help optimize an AWS environment for cost efficiency, performance, security, and fault tolerance. It analyzes an AWS account and offers recommendations based on best practices and AWS architectural principles. Trusted Advisor evaluates areas such as cost optimization, security, performance, and fault tolerance, providing actionable insights to improve the overall health of AWS resources. The service helps users proactively address issues, reduce costs, and enhance the security and performance of their AWS workloads. Trusted Advisor is available to AWS customers with a Business or Enterprise support plan and offers personalized recommendations to align with specific needs and usage patterns.

8. GuardDuty, CloudTrail, Inspector

Usage: Threat detection, activity logging, and vulnerability assessments.

Vulnerability Mitigation: Addresses absence of threat detection mechanisms and provides insights into security and compliance risks.

AWS Inspector

This service performs automated security assessments to identify compliance issues and vulnerabilities in AWS resources and applications. It helps in enhancing the security posture of the AWS environment.

AWS Guard Duty

AWS GuardDuty is a threat detection service in AWS that continuously monitors and analyzes the activity and behavior of AWS accounts. It uses machine learning algorithms and threat intelligence to identify and alert on potentially malicious activity, unauthorized behavior, and security risks. GuardDuty analyzes data from various AWS sources, such as CloudTrail logs, VPC Flow Logs, and DNS logs, to detect anomalies and potential security threats. It provides detailed findings and context about security incidents, enabling quick investigation and response. GuardDuty helps enhance the security posture of AWS environments by providing real-time threat detection and actionable insights to mitigate risks.

CloudTrail

This is one of the monitoring tools we deployed for our health care application to record API activities for better visibility and auditing of actions taken on AWS infrastructure and resources such as changes on EC2, RDS instances, creation or deletion of S3 bucket and objects in it, changes to IAM policies.

9. Elastic Load Balancer & VPN Gateway

Usage: Distributes incoming traffic and provides VPN connectivity.

Vulnerability Mitigation: Enhances network security, addressing weaknesses in load balancing and VPN connections.

Elastic Load Balancer

Amazon Elastic Load Balancer (ELB) in AWS is a service that automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses, within one or more availability zones. ELB enhances the availability and fault tolerance of applications by distributing traffic evenly and directing it away from unhealthy instances. It supports various load balancing algorithms and can automatically scale to adapt to changing traffic patterns. ELB provides a single point of contact for clients, improving the scalability and reliability of applications. Additionally, it integrates seamlessly with other AWS services, making it a key component in creating highly available and scalable architectures in the cloud.

VPN Gateway

An AWS VPN Gateway is a service that allows secure communication between an on-premises data center and Amazon Virtual Private Cloud (Amazon VPC). It facilitates the establishment of an encrypted and private connection, often using Internet Protocol Security (IPsec) protocols. The VPN Gateway enables organizations to extend their on-premises network to the AWS cloud securely, creating a hybrid IT environment. It supports both Site-to-Site VPN connections, connecting an on-premises network to a VPC, and Client VPN connections, allowing remote users to access resources in a VPC. VPN Gateway plays a crucial role in building a secure and scalable network architecture that spans both on-premises and cloud environments.

10. AWS Lambda & S3 Object Lambda Access Points

Usage: Serverless computing service and data processing at the time of retrieval from S3.
Vulnerability Mitigation: Enhances data processing security and reduces exposure to data breaches.

AWS Lambda

AWS Lambda is a serverless computing service in AWS that allows developers to run code without provisioning or managing servers. Users can upload their code, and Lambda automatically takes care of the underlying infrastructure, scaling the execution based on demand. Lambda supports multiple programming languages and event sources, allowing developers to build a wide range of applications, from simple scripts to event-driven microservices. It follows a pay-as-you-go pricing model, where users only pay for the compute time consumed by their code. Lambda integrates seamlessly with other AWS services, enabling developers to create powerful, scalable, and cost-effective applications.

S3 Object Lambda

Amazon S3 Object Lambda is a feature in AWS S3 that allows users to run custom code on S3 GET requests, transforming the data returned by the request. It enables dynamic and on-the-fly processing of S3 objects as they are retrieved, without having to modify the underlying data stored in S3. S3 Object Lambda functions are serverless and can be written in languages like Python or Node.js. This feature is particularly useful for scenarios where data transformation or filtering is required before delivering the object to the requester. S3 Object Lambda enhances the flexibility and agility of data processing workflows in S3, enabling users to apply custom logic during object retrieval.

11. Amazon S3 & S3 Snapshot Backup

Usage: Object storage service with backup capabilities.
V**ulnerability Mitigation:** Addresses data loss and recovery concerns, mitigating risks related to data breaches and accidental deletions.

Amazon S3
Amazon S3 (Simple Storage Service) in AWS is a scalable object storage service designed to store and retrieve any amount of data at any time. Users can upload and download data using the S3 web interface or through API calls. S3 offers high durability, availability, and low-latency access to stored objects, making it suitable for a wide range of use cases, from data archiving to serving static website content. S3 provides features such as versioning, server-side encryption, and access control policies to secure and manage data. Additionally, S3 is integrated with various AWS services, enabling seamless data storage and retrieval across the AWS ecosystem.

S3 Snapshot Backup
AWS S3 does not have a native snapshot backup feature like some other AWS services such as Amazon EBS (Elastic Block Store). In the context of S3, users typically achieve data backup by creating copies of their objects and storing them in the same or different S3 buckets. Versioning in S3 allows users to keep multiple versions of an object over time, acting as a form of historical backup. Additionally, users can implement lifecycle policies to transition older versions to lower-cost storage classes or to expire them after a specified period. While S3 itself doesn't have snapshots, users can build robust backup strategies using versioning, replication, and lifecycle policies to ensure data durability and availability.

12. AWS Backup

Usage: Centralized backup service across AWS services.
Vulnerability Mitigation: Ensures data integrity and availability, addressing backup and recovery vulnerabilities.

AWS Backup

AWS Backup is a fully managed backup service in AWS that centralizes and automates the backup of data across various AWS services. It supports backup of services like Amazon EBS, Amazon RDS, Amazon DynamoDB, and more. AWS Backup simplifies the creation, management, and retention of backups, providing a unified console to set up and monitor backup policies. It allows users to define backup plans, schedule backups, and automate backup lifecycle management. With AWS Backup, organizations can ensure data protection and compliance by implementing a consistent and centralized backup strategy across their AWS resources.

13. S3 VPC Endpoints & Internal Checkpoint Firewall

Usage: Securely connects VPCs to S3 and internal network protection.
Vulnerability Mitigation: Strengthens network security, addressing vulnerabilities related to insecure data transfers and internal network threats.

14. AWS Data Processing and Visualization Group (Amazon QuickSight, AWS Glue, Amazon EMR, Amazon Athena, Amazon Redshift, AWS Lake Formation)

Usage: Data processing, analysis, and visualization services.
Vulnerability Mitigation: Enhances monitoring and reporting capabilities, indirectly addressing various security vulnerabilities.

Amazon QuickSight
Amazon QuickSight is a cloud-powered business intelligence service by AWS. It enables users to create and share interactive dashboards with insights from various data sources. QuickSight supports ad-hoc analysis, data exploration, and embedded analytics for applications. It integrates seamlessly with other AWS services and on-premises databases. QuickSight's pay-per-session pricing model makes it cost-effective and scalable for organizations of all sizes.

AWS Glue
AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy to prepare and load data for analysis. It automatically discovers, catalogs, and transforms metadata from different sources, making data integration more straightforward. Glue supports various data formats and provides visual tools for ETL job authoring. It seamlessly integrates with other AWS services, such as S3, Redshift, and Athena. AWS Glue simplifies the ETL process, enabling users to build scalable and efficient data pipelines.

Amazon EMR (Elastic MapReduce)
Amazon EMR is a cloud-based big data platform that enables processing of large amounts of data quickly and cost-effectively.EMR utilizes popular frameworks like Apache Spark and Apache Hadoop for distributed data processing.It supports a wide range of applications and frameworks, making it versatile for various big data use cases. EMR instances can be easily scaled up or down based on processing requirements, integrated with other AWS services and allows seamless data transfer and analysis.

Amazon Athena
Amazon Athena is an interactive query service that enables users to analyze data in Amazon S3 using SQL.It requires no infrastructure setup or data loading, as it directly queries data stored in S3. Athena supports a variety of data formats and integrates

seamlessly with services like AWS Glue for schema discovery. It provides fast query performance and is suitable for ad-hoc querying and analysis. Athena is a serverless and cost-effective solution for querying data in the data lake stored in Amazon S3.

Amazon Redshift

Amazon Redshift is a fully managed data warehouse service designed for high-performance analysis using SQL queries. It is optimized for large datasets and supports petabyte-scale data warehouses. Redshift offers fast query performance through advanced compression techniques and columnar storage. It seamlessly integrates with other AWS services and supports popular BI tools. Redshift's scaling capabilities make it suitable for a wide range of analytics and reporting applications.

AWS Lake Formation

AWS Lake Formation simplifies the process of setting up, securing, and managing a data lake.It provides tools for ingesting, cataloging, and transforming data to make it available for analytics. Lake Formation automates tasks like data deduplication, format normalization, and access control. It integrates with various AWS services, allowing users to build scalable and secure data lakes. Lake Formation streamlines data lake management, making it easier for organizations to derive insights from their data.

15. Amazon RDS, DynamoDB, QLDB

Usage: Database services for structured and unstructured data.
Vulnerability Mitigation: Addresses database security vulnerabilities, ensuring data integrity and security.

Amazon RDS (Relational Database Service)

Amazon RDS is a managed relational database service that supports popular database engines like MySQL, PostgreSQL, Oracle, SQL Server, and MariaDB. It automates routine database tasks such as hardware provisioning, database setup, patching, and backups, allowing users to focus on application development. DS provides high availability, automatic backups, and scaling capabilities to meet the performance requirements of various applications. It offers features like Multi-AZ deployments for fault tolerance and Read Replicas for improved read performance. RDS is a suitable choice for applications that require a traditional relational database structure.

Amazon DynamoDB

Amazon DynamoDB is a fully managed NoSQL database service designed for high-performance, low-latency applications. It provides seamless scalability, enabling users to handle varying workloads with automatic partitioning and distribution. DynamoDB offers features like on-demand and provisioned capacity, global secondary indexes, and built-in security controls. It is well-suited for use cases requiring fast and predictable performance, such as real-time applications and serverless architectures. DynamoDB integrates with AWS services and SDKs, making it easy to develop applications with a variety of programming languages.

Amazon QLDB (Quantum Ledger Database)

Amazon QLDB is a fully managed ledger database service designed to provide transparent and immutable transaction log capabilities. It offers a centralized, cryptographically verifiable transaction history that makes it suitable for applications requiring an authoritative and tamper-resistant record of changes' uses a purpose-built, serverless architecture for scalable and cost-effective ledger applications. It supports a familiar SQL-like query language for easy integration with existing applications' is particularly useful for scenarios such as financial services, supply chain, and other applications that require an auditable and tamper-proof transaction history.

16. AWS Global Services & Site-to-Site VPN

Usage: Global cloud services and secure site-to-site VPN connections.
Vulnerability Mitigation: Enhances global connectivity and secure data transfer between sites.

AWS Global Services are designed to provide a consistent and reliable experience to users worldwide. This ensures that organizations can deploy applications and services globally, reaching end-users with low latency and high availability.

Site-to-Site VPN connections establish encrypted tunnels over the public internet, securing data in transit between on-premises locations and the AWS cloud. This mitigates the risk of data interception or unauthorized access during transit.

17. PaloAlto Firewalls & Barracuda WAF

Usage: Advanced firewall and web application firewall for network security.
Vulnerability Mitigation: Addresses vulnerabilities in network firewall configurations and web application security.

PaloAlto Firewalls in AWS

PaloAlto Networks provides next-generation firewalls that play a crucial role in securing AWS environments. PaloAlto firewalls offer advanced threat prevention features, including intrusion detection and prevention, URL filtering, and application awareness. In AWS, PaloAlto firewalls help enforce security policies, monitor network traffic, and protect against various cyber threats. They provide visibility into application and user behavior, allowing for granular control and threat mitigation. PaloAlto firewalls can be seamlessly integrated into AWS architectures to enhance the overall security posture of cloud-based applications and data.

Barracuda WAF (Web Application Firewall) in AWS

Barracuda WAF is designed to protect web applications from various cyber threats and attacks. In AWS, Barracuda WAF acts as a security gateway, monitoring and filtering HTTP traffic between web applications and the internet. It provides features such as web application security, protection against OWASP Top 10 vulnerabilities, and bot mitigation. Barracuda WAF helps secure applications running in AWS by identifying and blocking malicious traffic before it reaches the web servers. It offers centralized management, real-time threat intelligence, and logging capabilities to enhance the security of web applications in the cloud.

18. Amazon EBS & Auto Scaling

Usage: Block storage for EC2 and automatic adjustment of computing resources.
Vulnerability Mitigation: Ensures data security on EC2 instances and resilience in resource allocation.

Amazon EBS (Elastic Block Store)
Amazon EBS is a block-level storage service in AWS that provides durable and scalable block storage volumes for use with EC2 instances.EBS volumes are highly available and can be attached to EC2 instances to provide additional storage capacity. It supports various volume types, including General Purpose SSD, Provisioned IOPS SSD, and Magnetic, each optimized for different performance characteristics.EBS volumes can be easily backed up, snapshotted, and resized, offering flexibility in managing data storage for EC2 instances. EBS plays a critical role in providing persistent and high-performance storage for EC2 workloads in AWS.

Auto Scaling in AWS
Auto Scaling is a service that automatically adjusts the number of EC2 instances in an Auto Scaling Group based on demand or a defined schedule. It helps ensure the availability and reliability of applications by dynamically adjusting capacity to handle varying workloads. Auto Scaling can scale instances in and out based on metrics such as CPU utilization, network traffic, or custom metrics. It integrates with other AWS services, enabling seamless scaling for applications across multiple availability zones. Auto Scaling enhances the efficiency and cost-effectiveness of applications by automatically managing the compute capacity required to maintain performance.

19. EC2 Instances & Interface VPC Endpoint

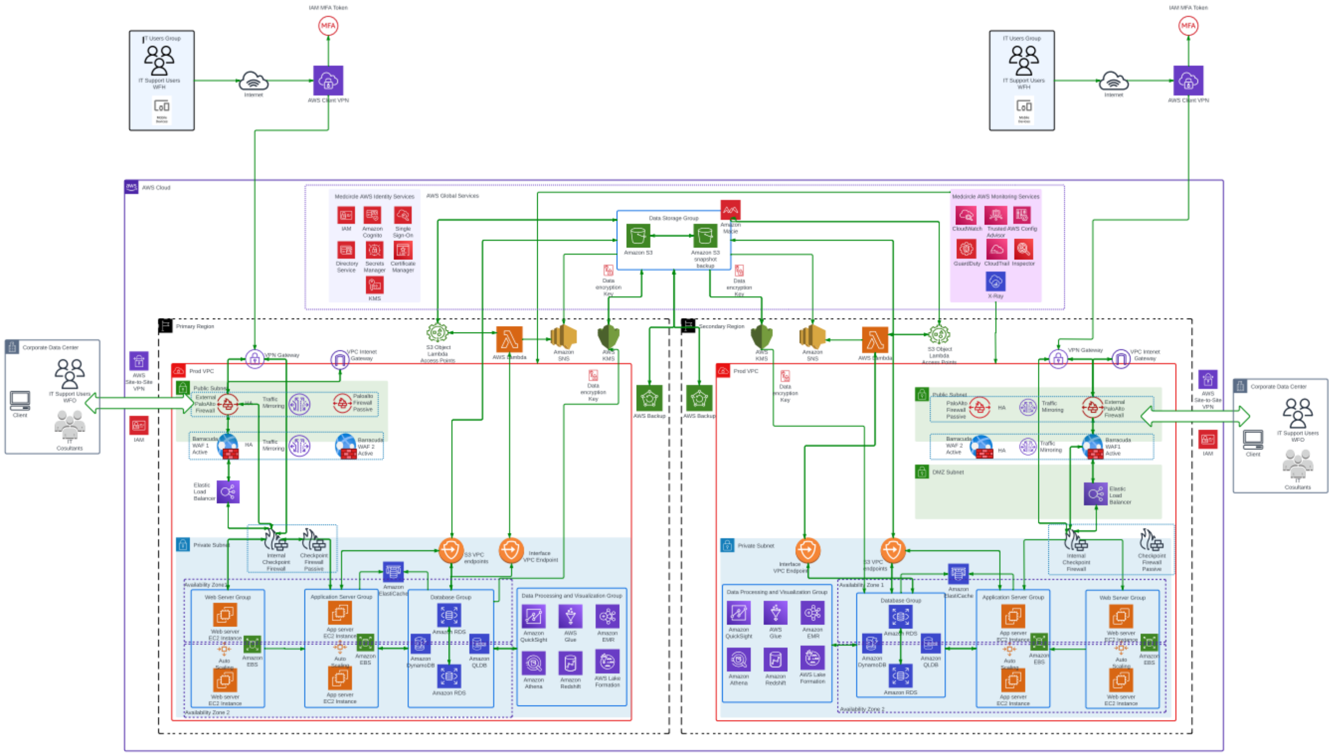
Usage: Virtual servers in the cloud and private connectivity to AWS services.
Vulnerability Mitigation: Addresses EC2 security concerns and ensures secure access to AWS services.

EC2 security concerns can include unauthorized access, data breaches, and vulnerabilities in the operating system or applications running on instances. Properly configuring security groups, network ACLs, and implementing secure access controls helps mitigate these concerns.Interface VPC Endpoints enhance security by allowing private communication between EC2 instances and AWS services. This eliminates the need for internet-facing gateways, reducing the attack surface and exposure to potential threats.

Architecture Details- IT support view

The Medicare hospital's IT infrastructure is a highly integrated and secure setup, designed to meet healthcare industry needs. It features multiple segregated Virtual Private Clouds (VPCs) for different operational environments, employs a suite of AWS services for data processing and storage, and prioritizes security and compliance with tools like Barracuda WAF, PaloAlto, Checkpoint Network Firewalls, adhering to HIPAA standards. The infrastructure is built for resilience with active-passive redundancy across regions and employs AWS Client VPN with multi-factor authentication for secure access for IT personnel.

Architectural Design – IT Employee View



Link to Lucid chat- <u>AWS Architecture Diagram - IT Employess View</u>

In our infrastructure, IT employees operate within dedicated IP schemas/VLANs, ensuring network segregation and enhanced security. Remote employees access AWS via a Remote Access VPN (AWS VPN Client) with AES-256 encryption, whereas office employees use a Site-to-Site (S2S) VPN tunnel. Remote traffic reaches the external Palo Alto firewall via a VPN gateway; office traffic is directly routed to the external firewall, then into the AWS VPC. Within the VPC, services are meticulously organized: Identity Services, Monitoring Services, and others dedicated to Servers, Databases, and Storage, each segmented for operational efficiency and security. This architecture facilitates secure, role-based access control and maintains robust network integrity.

Data Flow:

Access and Authentication:

Here we are considering 2 scenarios.

1. IT Employees working from home.
2. IT Employees working from office.

IT staff working from remote locations access the network via AWS Client VPN, using IAM MFA tokens for secure authentication. This ensures a secure entry point into the hospital's network, regardless of the user's location. Then the IP is allocated from the Employee access pool.

VPC NAT Gateway converts incoming public IP addresses to their respective private IP addresses and will forward the traffic to external firewall.

IT employees and other third-party support consultants working from the office connect to the AWS network via a Site-to-Site (S2S) VPN tunnel. This setup ensures that office-based IT personnel have a secure and encrypted pathway to the network.

"MedCircle Identity Services" are used to authenticate and authorize the user and control access. As mentioned, in both cases the traffic will reach the external PaloAlto firewall.

Adding the layers of security:

We used PaloAlto next generation firewall as our external firewall, which offers advanced network security features, such as Advanced Threat Prevention, Traffic Visibility and Control, Intrusion Prevention System (IPS), Application Control, URL Filtering, Threat Intelligence Integration, Sandboxing, User Identification and Control, VPN Support, High Availability and Scalability etc. to protect the network from unauthorized access and other cyber threats.

We have configured our Pal Alto Networks' firewalls in an active/passive high availability (HA) setup to ensure continuous network protection, uptime and availability.

As this is the internal traffic (trusted) it will not route to any WAF, it will take the interface that is directly connecting to internal checkpoint firewall.

We have used checkpoint firewalls as our internal firewalls which provide robust security architecture defending the network from intrusions, malware, and other cyber threats while facilitating secure data transfer and communication within the network.

We have configured our internal firewalls in an active standby mode.

Infrastructure Processing and Resource Management:
Elastic Load Balancers, web and application servers, RDS instances, Lambda functions, S3 buckets, EBS, EFS, and Elastic Cache are employed to handle administrator commands efficiently. EC2 server instances, part of an auto-scaling group, effectively manage peak workloads.

These EC2 instances utilize EBS for dynamic scaling of block storage space, ensuring sufficient and adaptable storage for system, application, and server files, thereby enhancing overall storage management and processing capabilities in our infrastructure.

Data Processing:
AWS services such as RDS, Lambda, S3, and EFS are utilized for data processing and storage.
The architecture supports secure handling and storage of sensitive patient data, in compliance with HIPAA standards.

Data Backup:
The backup strategy involves executing full and incremental backups across multiple regions and availability zones. This robust approach is likely facilitated by AWS services such as Amazon S3 for secure storage, AWS Backup for managing backup processes, and possibly Amazon RDS for database-specific backups. These services ensure that your data is securely backed up and can be recovered efficiently, providing a resilient and reliable backup system across your AWS environment.

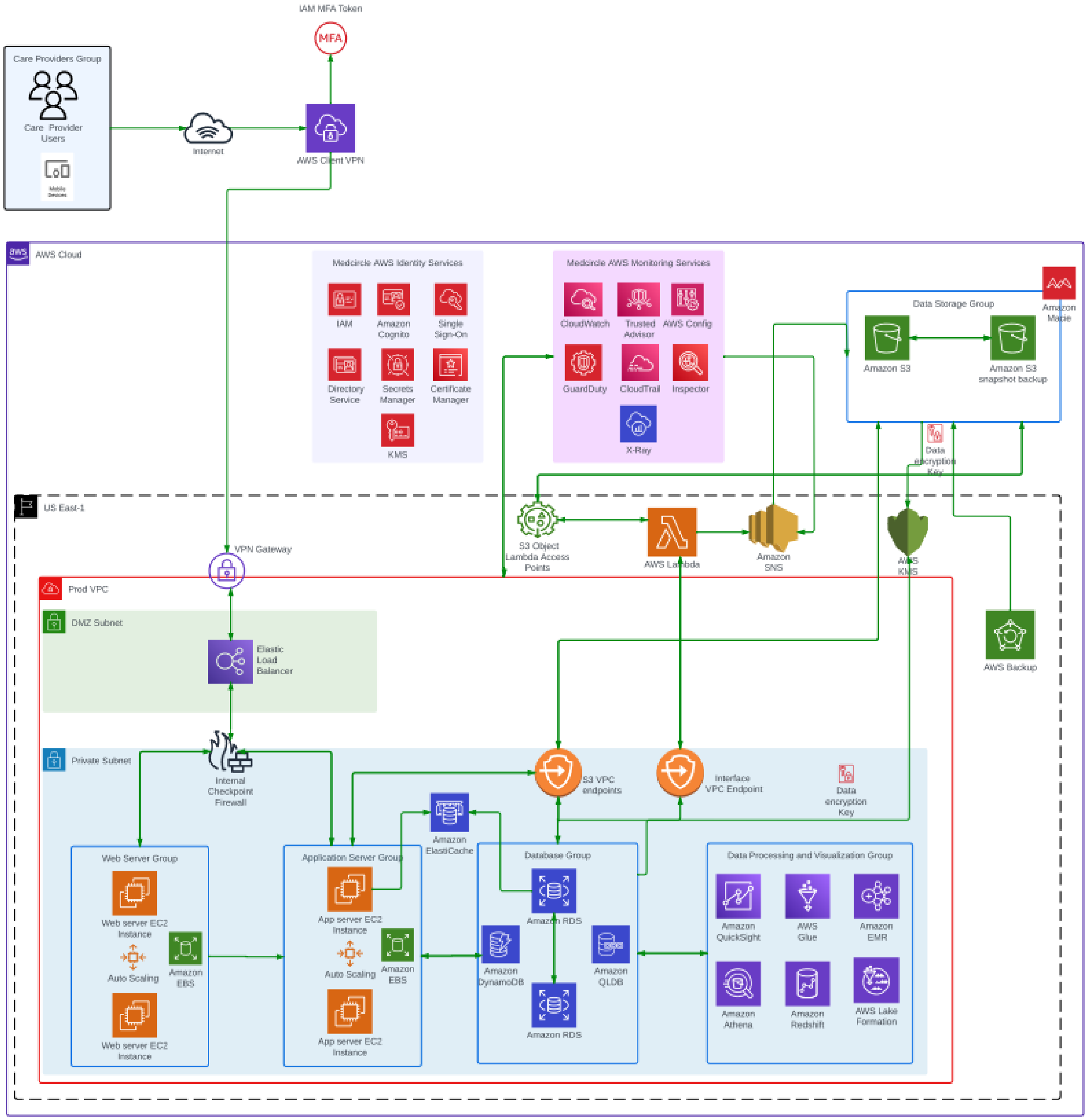
I**dentity Services:**
The infrastructure employs various identity services, crucial for security and access control. Some of them include AWS IAM (Identity and Access Management) for managing user access and permissions, and Amazon Cognito for user authentication and identity federation across web and mobile applications. AWS IAM is central to defining who can access which resources, ensuring secure and controlled access. Amazon Cognito simplifies user sign-up, sign-in, and access management, enhancing user experience and security.

Monitoring Services:
Various monitoring services are in place in our infra, services like AWS CloudWatch and AWS GuardDuty play vital roles. CloudWatch monitors and manages AWS resources and applications, providing data and actionable insights to optimize performance and resource utilization. GuardDuty offers threat detection, continuously monitoring for malicious or unauthorized behavior, safeguarding your infrastructure from potential security breaches. Together, these services ensure operational efficiency and robust security, enabling proactive management of resources and security threats in your AWS environment.

Effective Patch Management Strategy:

We have employed many AWS services and technologies to implement patch management. As part of this procedure, all servers, systems, and software components are routinely updated and secured. To ensure that systems are secure and up to date, automated patching is done using AWS Systems Manager. This approach is essential for protecting against vulnerabilities and guaranteeing adherence to the most recent security standards, all while preserving the integrity, security, and functionality of our IT system.

Architecture Details- Care Provider view



Link to Lucid chat- Care Provider View

The infrastructure includes various healthcare professionals such as doctors, nurses, lab technicians, pharmacy staff, receptionists, and in-house insurance providers. These individuals are responsible for both entering and accessing detailed patient information, ensuring comprehensive data management in the healthcare system. They need write access to Amazon RDS and S3 for storing patient data and scheduling appointments. For viewing and downloading other data, they require access to EC2 instances, Elastic Load Balancing, and other AWS resources. Additionally, AWS IAM manages identity for security, while AWS CloudWatch and AWS Lambda support monitoring and data processing. This arrangement ensures secure, efficient handling of patient data and communication with external entities like hospitals.

Traffic Flow and Data Management

- Requests entering through AWS Client VPN, ensuring secure and encrypted access.
- Traffic then routes through AWS VPN Gateway.
- MedCircle AWS Identity Services, including IAM, Amazon Cognito, and Directory Service, authenticate and authorize these requests.
- Data processing tools like AWS Lambda, Amazon S3, and Amazon RDS handle data storage and management.
- For visualization and analytics, requests may interact with Amazon QuickSight and AWS Glue.
- AWS CloudWatch and GuardDuty monitor this traffic, ensuring security and compliance.

Data Input and Automation in Healthcare:
Using Amazon RDS and DynamoDB, care providers input comprehensive patient data. Amazon RDS offers robust database management for structured data, while DynamoDB handles unstructured or semi-structured data, ensuring versatile data storage. AWS Lambda streamlines scheduling appointments and other automated tasks, enhancing operational efficiency.

Enhancing Healthcare Communication:
Secure communication, crucial for exchanging patient information and coordinating with external entities like hospitals, is facilitated by Amazon SNS and SES. These services offer reliable messaging and email capabilities, ensuring timely and secure exchanges.

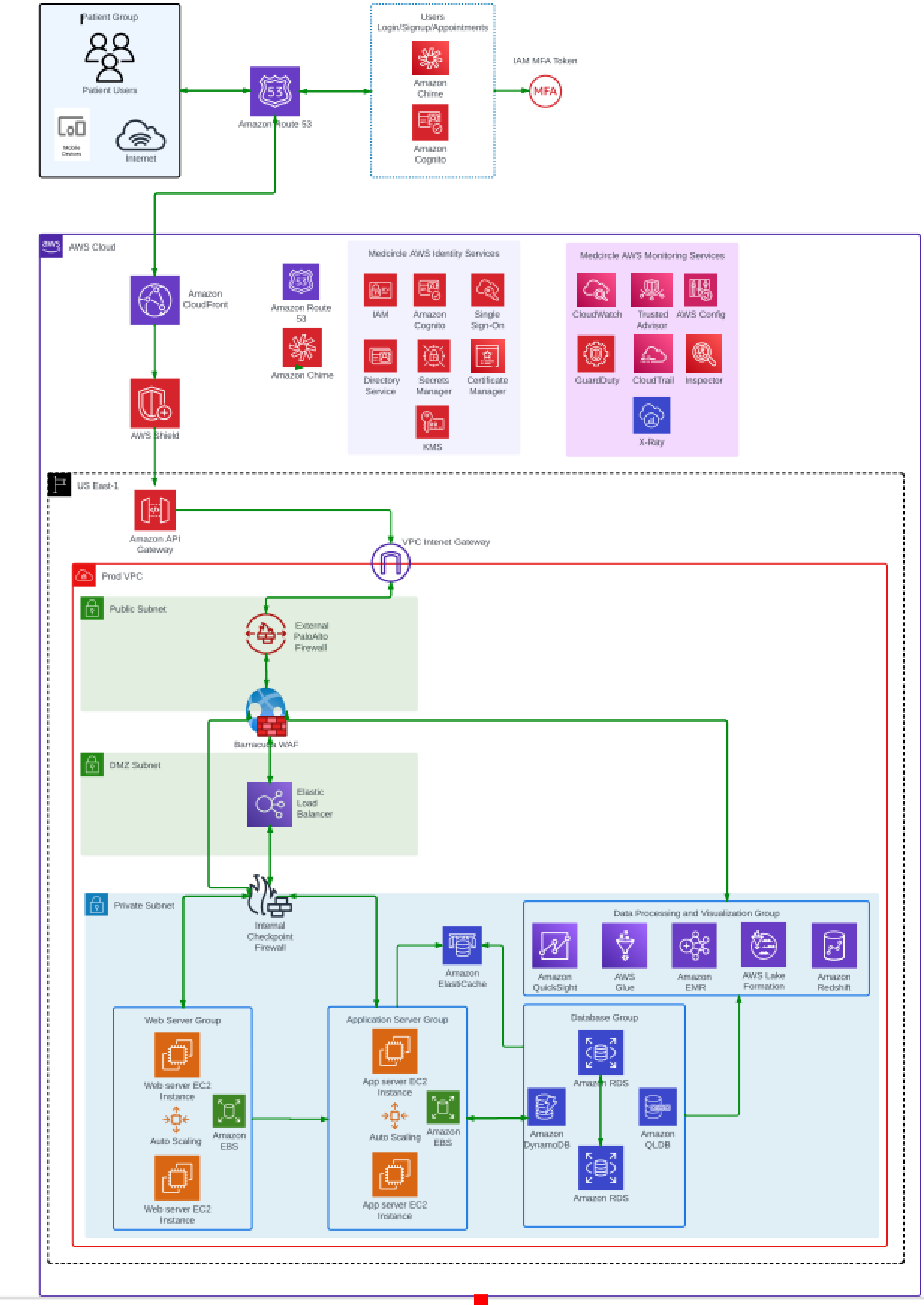
Data Access: Amazon S3 and EC2 instances provide secure and scalable data storage and retrieval solutions. They are helpful for accessing patient records, test results, and other critical medical data, supporting data-intensive healthcare operations.

Monitoring and Compliance: Continuous monitoring with AWS CloudWatch and GuardDuty is crucial for security and system health, while AWS Config helps maintain compliance with healthcare regulations, ensuring the infrastructure adheres to industry standards and protects patient data.

Data Analysis: Advanced data analysis is possible with Amazon QuickSight and Athena, providing insights into test results and patient data, which is key for informed medical decision-making and improving patient care outcomes.

Patient Interaction and Management: Enhancing patient interaction and communication, Amazon Connect and Amazon Pinpoint could be used for efficient appointment scheduling, reminders, and follow-up communications, streamlining patient management and improving the overall patient experience.

Architecture Details- Patient view



Link to Lucid chat - Patients View

Patients accessing our system from external sources via the internet benefit from a robust security infrastructure. We've established a user-friendly portal for patient login and signup, supported by Identity and Access Management (IAM) services for identity verification. SSL certificate management ensures secure communication. CloudFront, strategically positioned, accelerates content delivery to personal devices, enhancing user experience.

To safeguard against external threats, we prioritize security at every step. Incoming internet traffic undergoes stringent protection through AWS Shield, guarding against DDoS attacks. It then traverses Amazon API Gateway and an internet gateway to enter our Virtual Private Cloud (VPC).

At the VPC boundary, an external Palo Alto firewall plays a pivotal role. Configured for active-passive high availability, it ensures continuous protection and efficient traffic management. Following this, traffic is directed to the Barracuda Web Application Firewall (WAF) for defense against web-based threats.

Further down the chain, Network Address Translation (NAT) is applied, and traffic is passed to an internal firewall, bolstering security within the network.

To fulfill patient requirements, our architecture employs various AWS services, including Elastic Compute Cloud (EC2) instances for web and application hosting, Amazon RDS and DynamoDB for robust data storage, and a range of data processing and visualization services such as Amazon ElastiCache, QuickSight, Glue, EMR, Lake Formation, and Redshift.

Patients can easily access their test results via the web portal, which directs traffic through Barracuda WAF to our Data Processing Group. Here, AWS services like Amazon ElastiCache, QuickSight, Glue, EMR, Lake Formation, and Redshift are utilized to process and display the results

This comprehensive architecture ensures that patients can securely participate in telemedicine consultations, access test results, schedule appointments, and make general inquiries while maintaining the highest standards of security and data privacy.

Data Flow:

Patient Group and Device Access: Patients access the portal using personal devices (e.g., smartphones, tablets, laptops). This requires a secure, user-friendly interface.

Amazon Route 53: This is used for DNS management, ensuring that the web portal is easily accessible and reliable.

Identity and Access Management (IAM) and Amazon Cognito: These services manage user identities and authentication. IAM ensures secure access control to AWS services, while Cognito provides user sign-up, sign-in, and access control to the web application. Multi-factor authentication (MFA) enhances security.

AWS CloudFront: As a content delivery network (CDN), CloudFront speeds up the distribution of your web portal content. It's correctly placed at the edge of the network to cache content closer to users, reducing latency and improving user experience.

AWS Shield and Amazon API Gateway: AWS Shield provides DDoS protection. The traffic is first routed through AWS Shield for security screening before reaching the API Gateway, which acts as the front door for all requests to backend services.

VPC and Internet Gateway: The Virtual Private Cloud (VPC) isolates your network infrastructure. The Internet Gateway allows communication between your VPC and the internet.

Palo Alto Firewall (External): Positioned in the DMZ subnet, this firewall provides an additional layer of security against external threats. Configured in an active-passive high availability mode, it ensures continuous network protection and traffic management without downtime.

Barracuda Web Application Firewall (WAF): It protects the web application from common exploits and vulnerabilities. Barracuda WAF filters and monitors HTTP traffic between the internet and your application, offering protection against SQL injection, cross-site scripting, and other web-based attacks.

Internal Check Point Firewall: This internal firewall provides another security layer within the AWS environment, ensuring that only authorized traffic reaches your internal network.

Web and Application Server Groups: Hosted on EC2 instances with auto-scaling and Elastic Block Store (EBS), these servers handle the web portal and application processing.

Data Processing and Visualization Group: Utilizes AWS services like Amazon ElastiCache, QuickSight, Glue, EMR, Lake Formation, and Redshift for data storage, processing, and visualization. These services enable patients to access their test results directly through the web portal.

Database Group: Comprises Amazon RDS, DynamoDB, and QLDB for robust data storage and management.

Monitoring Services: AWS CloudWatch, Config, GuardDuty, CloudTrail, Inspector, and X-Ray provide monitoring, logging, and compliance checks. These services ensure the operational health and security of the entire infrastructure.

Conclusion

It emphasizes the successful implementation of a robust, secure, and efficient IT infrastructure for a healthcare application using AWS. It highlights the major improvements made in various aspects such as security protocols, IAM, disaster recovery, data encryption, and network security. The document concludes with confidence in the enhanced security, compliance, and operational efficiency achieved through these upgrades.

References:

1. https://aws.amazon.com/blogs/database/demystifying-amazon-rds-backup-storage-costs/
2. https://aws.amazon.com/s3/faqs/
3. https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReplicateBa
4. ckups.html
5. https://aws.amazon.com/blogs/security/aws-becomes-first-cloud-service-provider-to-adopt-new-pci-dss-3-2/
6. https://aws.amazon.com/guardduty/
7. https://docs.aws.amazon.com/waf/latest/developerguide/waf-chapter.html
8. https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html
9. https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-groups.html
10. https://aws.amazon.com/cloudwatch/
11. https://docs.aws.amazon.com/managedservices/latest/userguide/comprehend.html
12. https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html#
13. https://mindmajix.com/top-aws-services
14. https://www.geeksforgeeks.org/top-aws-services