MEGA We care

Website System Architecture and Security Overview

This document explains how **“Mega We care”** websites use the hosting provider, cloud infrastructure, backend services, databases, backups, third party tools and security measures in place to ensure a reliable and secure environment.

1. Shared Responsibility Model

Mega We Care’s websites follow a shared responsibility model, where security, reliability, and availability are not handled by a single party but are shared across multiple layers.

Infrastructure providers

Cloudflare, AWS, and MongoDB Atlas Cloud are responsible for securing the cloud platforms, networks, and environments they operate.

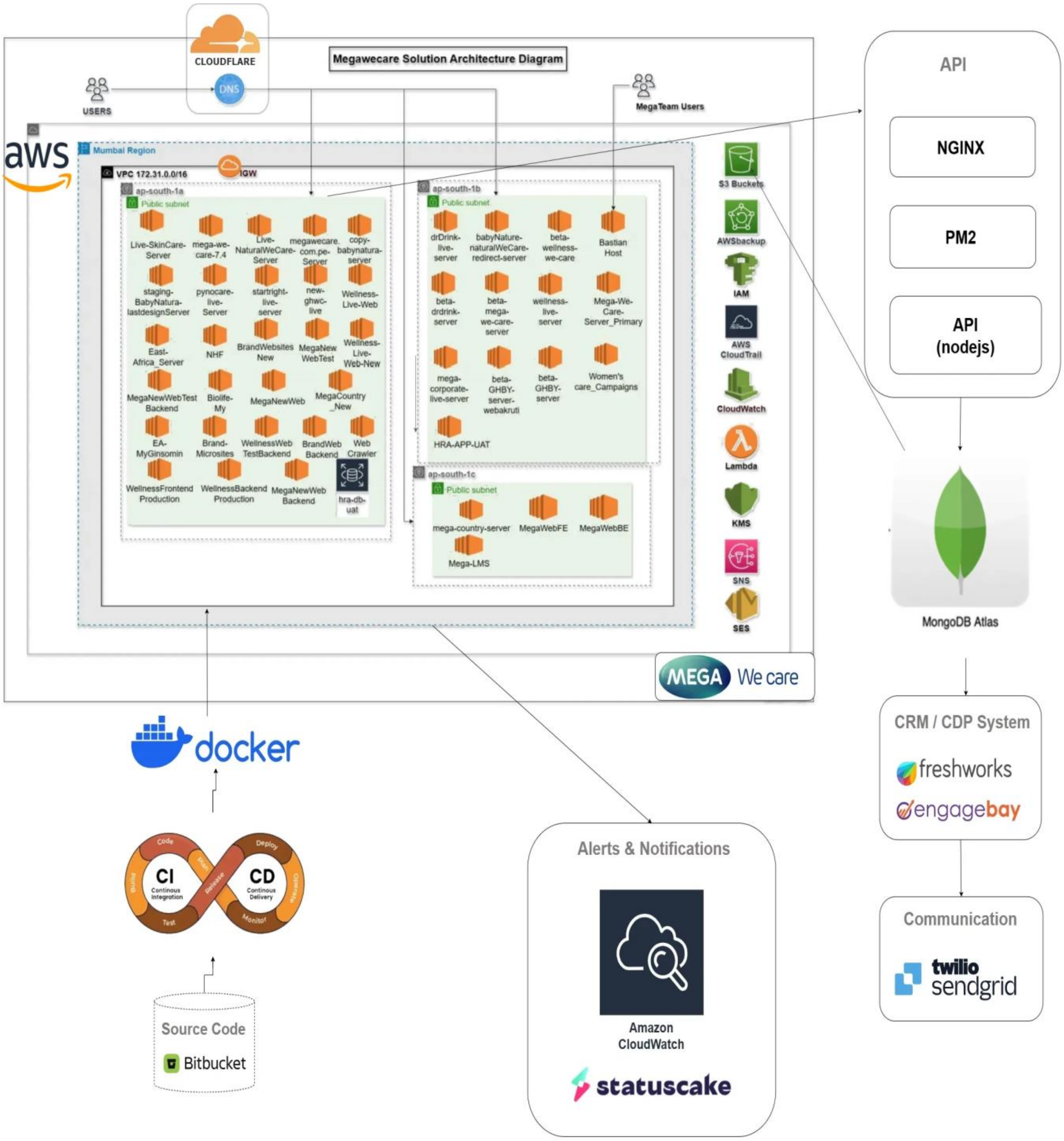
Development Team

The Development Team is responsible for securely designing, configuring, and managing how these platforms are used within the application.

Business platforms

Third party CDP/ CRM tools Freshworks and EngageBay are responsible for securing their services and protecting the customer data stored within their systems.

2. Architecture and Data Flow



3. Security and Edge Services

All user traffic first reaches through **Cloudflare**, a global network that acts as our first line of defense and hosting provider.

3.1 Cloudflare: Edge Network & Hosting (The Entry Point)

Cloudflare process incoming requests to ensure the security of websites by providing

- **SSL/TLS Encryption:** Encrypts all data between users and the website, so information cannot be read or altered during transmission.
- **DDoS Protection:** Automatically detects and blocks large-scale traffic attacks that try to overload and take the website offline.
- **Web Application Firewall (WAF):** Filters and block malicious requests such as hacking attempts, SQL injection, and other common web attacks before they reach the servers.
- **Bot Protection:** Identifies and stops harmful automated bots while allowing real users and trusted services to access the website.
- **API Shield:** Protects backend APIs by detecting abnormal or unauthorized API requests and reducing the risk of API abuse or exploitation.
- **Global Cache (CDN):** Serves static website content from Cloudflare's global network, reducing load on backend servers, lowering response time, and improving website performance.

3.2 Amazon Web Services (AWS): Cloud Infrastructure

AWS services work together to secure the website by controlling access, encrypting data, monitoring activity, and sending alerts, ensuring a secure, reliable, and highly available system.

The AWS services used are listed below:

- AWS IAM
- AWS CloudTrail
- Amazon CloudWatch
- Amazon SNS (Simple Notification Service)
- AWS Key Management Service (KMS)

4. Application Gateway

After traffic passes through **Cloudflare and AWS**, it reaches **NGINX** on the application server. **NGINX** secures the system by controlling access to internal services and it also

- Enforces secure **HTTPS** access.
- Blocks **invalid or abusive** requests.
- Limits **excessive connections** and helps **prevent resource-exhaustion attacks**.

5. Backend Services

We use **Node.js** with **Express.js** to build RESTful APIs that handle all backend operations and data communication for the system.

Security is enforced using **JWT (JSON Web Token)–based authentication**, where only authenticated and authorized users can access **backend API services** through a verified token. This prevents unauthorized access and protects data from being read or modified by attackers.

6. Database Storage

We have used **MongoDB (NoSQL)** as the database for our websites to store all website content and related data. It is hosted on **MongoDB Atlas Cloud**, a fully managed platform that ensures security, scalability, and reliable performance.

7. Deployment and Updates

All website source codes are stored in **Bitbucket** using separate repositories to manage versions and updates safely. A **CI/CD (Continuous Integration and Continuous Deployment) pipeline** is used to automatically build, test, and deploy code changes, enabling faster and reliable updates.

Docker-based containerization ensures the application runs consistently across all environments, allowing smooth deployments and continuous updates while keeping the website stable and available.

8. Backup and Recovery

We follow a structured backup strategy for our infrastructure, databases, source code, and critical data using automated and manual processes. Backups are maintained on secure cloud and local storage with regular schedules to ensure data availability and redundancy.

Area	Backup Type	Frequency	Where is it stored?
Website Data (Mega Corporate, Mega Country, Brand Websites, Wellness We care, Women We care, Medical Nutrition and Mother We care)	**Cloud**	**Daily**	**AWS Backup Services**
Database (Mega Corporate, Mega Country, Brand Websites, Wellness We care, Women We care, Medical Nutrition and Mother We care)	**Cloud + Local Machine**	**Daily + Monthly**	**Mongo DB Atlas Cloud & AWS S3 Bucket**
Files & Media	**Cloud + Local Machine**	**Daily + Weekly**	**AWS S3 Bucket and on Local Machine**
Server (Other Website and its Database)	**Cloud**	**Daily + Weekly**	**AWS Backup Services**
Website Code (Mega Corporate, Mega Country, Brand Websites, Wellness We care, Women We care, Medical Nutrition and Mother We care)	**Version Control + Local Machine**	**Continuous**	**Bitbucket Repository and on Local Machine**

9. Alert and Notifications Services

We have used **AWS CloudWatch** which helps to monitor website infrastructure and trigger real-time email and SMS alerts for critical issues, enabling quick responses and minimizing downtime.

Additionally, we use **StatusCake**, a third-party monitoring service, to independently track website availability. It sends real-time alerts if the website becomes unavailable, ensuring faster issue detection and improved service reliability.

10. CRM / CDP Marketing Tools

We have used **Third Party CRM/CDP platforms,** i.e **Freshworks and EngageBay** which stores and manages customer interactions such as support chats and email communications. Customer data is shared only with user consent and limited to the minimum required for business purposes.

Access to these platforms is restricted to authorized users through secure authentication and access controls, ensuring customer data privacy, and preventing unauthorized access.

11. Communication Services

To communicate with customers, we have used **SendGrid** and **Twilio Email Services** to send automated and transactional emails.

These services are used to deliver thank-you emails for newsletter subscriptions, calculator usage, comments and replies, contact form submissions, expert queries, health test requests, and other form-based interactions from the websites.