membrance®
Live Forever Digitally

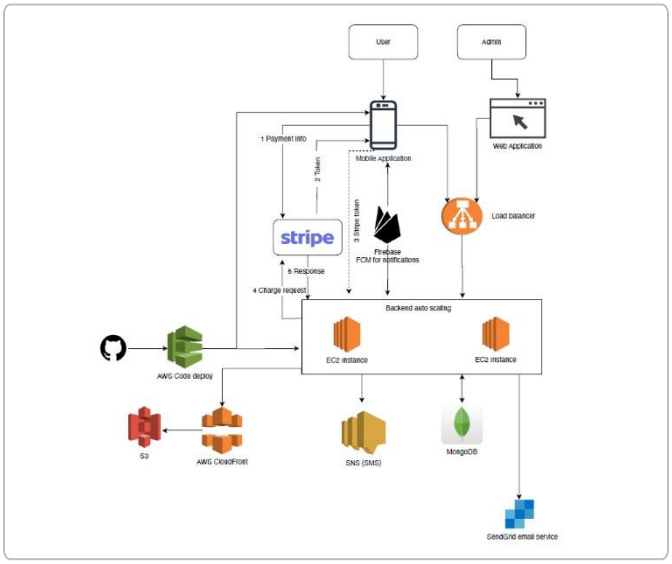
# Security and Infrastructure

Membrance Inc. has incorporated industry leading security standards into the development of our software platform architecture, designed with multiple layers of protection, covering data transfer, encryption, network configuration, and application-level control, all distributed across a scalable secure infrastructure that ensures consumer data and where it resides, utilizes the latest technology and processes, to guarantee safety, security and perpetuity.

## Built for "Peace of Mind Beyond a Lifetime"

- AWS Perpetual Hosting: The world's most comprehensive and broadly adopted cloud that includes infrastructure as a service (IaaS) and platform as a service (PaaS) with an Instance-Level SLA Uptime of at least 99.99%.
- Multi-Factor Authentication: Access to our application is secured through a multi-step login process, requiring additional verification factors as part of a comprehensive identity and access management (IAM) policy.
- AES-256 Data Encryption: Widely considered the most secure encryption available today, all user data is converted into a cipher through a virtually impenetrable symmetric encryption algorithm using a 256-bit key.
- Automated Content Moderation: Real-time detection of inappropriate content including nudity, blood, violence, weapons, self-harm and more utilizing state-of-the-art models, capable of analyzing video faster than humans.

## Architecture Diagram




## Monitoring

Membrance and AWS (our hosting provider) utilize a wide variety of automated monitoring systems to provide a high level of service performance and availability. Monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. The tools have the ability to set custom performance metrics thresholds for unusual activity.

## Physical Security

AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in, continually escorted by authorized staff.

## Intrusion Detection

Intrusion Detection Systems (IDS) are deployed throughout Membrance infrastructure. The systems are configured to identify malware infections, attacks, system compromises, policy violations, and other exposures, alerting administrators to take immediate action of potential intrusions by analyzing network traffic and system activity.

## Software Stack

amazon web services · sightengine · GitHub · tiny · mongoDB · twilio · Firebase · stripe