cureatr

Cureatr System and Security Overview

Last updated: August 21, 2019

cureatr

The Cureatr System

Cureatr is Software as Service (SaaS) application, built from the ground up as a scalable and highly available cloud-based service. This paper explains how the Cureatr cloud application is built – with scalability and availability at its core.

Architecture

Cureatr is a secure cloud-based application residing on Amazon Web Services (AWS) Virtual Private Cloud (VPC) as the hardware virtualization layer. Users access Cureatr on a mobile device or an application running in a web browser, which communicate to the Cureatr backend via Application Programming Interfaces (APIs).

Supported Devices & Browsers

- iOS – version 11.0 or above
  - The app is compatible with iPhone, iPod Touch, and iPad.
- Android – version 6 or above
  - The app is compatible with the majority of Android devices.
- Web
  - Microsoft Internet Explorer version 11 (desktop)
  - Apple Safari last 3 versions (desktop and iPad)
  - Google Chrome last 3 versions (desktop)

Security & Encryption Details

In the following sections we explain how we address security starting at the devices that the application is installed on, to the data in transit between the user and AWS, and ultimately within AWS.

cureatr

Device Security

Mobile Devices – iOS and Android

- Data is encrypted any time we write it out to local storage, in which we cache most recent messages as well as attachments to allow them to be accessed faster when the application is opened.
- We use AES-256 symmetric key encryption for all local data, and store the unique per-user key in the user's record on our servers, where the key itself is stored encrypted. Only Cureatr mobile apps that have a valid authenticated session can retrieve the key from our servers and decrypt local data.
- Device administrators can reset each user's key, effectively performing a remote wipe. This functionality is independent of any system wipe through methods provided by the iOS or Android systems.

Device Access

- Cureatr requires that all devices be locked with a 4+ digit passcode or fingerprint authentication on iOS or a 4+ digit passcode, pattern lock, or fingerprint authentication on Android devices.
- Customers have a choice of requiring an application passcode to be used for all users.
- If the device has MDM software that enforces device security requirements, the Cureatr application will not conflict with it in any way.
- The user can configure a timeout period before the passcode must be entered. The maximum timeout period is 15 minutes.

Account Password

- Cureatr account passwords must be at least 8 characters long, and must contain one uppercase letter, one lowercase letter, and one number or special character.
- The in-app timeout before the user must sign in again is 72 hours of inactivity.
- Cureatr apps have full support for SAML 2.0 and OIDC Single Sign On with enterprise Identity Providers, and we encourage all customers to utilize that functionality.
- Cureatr system and customer operations administrators are required to use two-factor authentication to access production systems or administrative applications.


cureatr

cureatr

Data In Transit

All data in transit is encrypted. All communication with Cureatr servers goes over HTTPS/SSL. The currently supported protocol is TLSv1.2 and the enabled ciphers are the ones recommended by the latest high security settings.

Amazon Web Services (AWS)

Cureatr maintains a Business Associate Agreement with AWS and uses only services that have been labeled as BAA-compatible with AWS. Cureatr follows AWS guidelines for designing and building secure applications on top of the AWS platform.

Data Storage

- Cureatr database servers utilize encrypted EBS file systems for data storage, with key management provided by the AWS Key Management Service.
- When data that arrived on the server needs to be written to the database, wherever possible sensitive fields are further encrypted at the field level with AES-256 symmetric key encryption to provide additional protection.
- The master keys for database encryption are stored in "protected packages" that keep all the sensitive data needed by our applications.
- Starting any application server or tool that accesses sensitive data requires the protected package to be unlocked. This means the authorized administrator needs to enter their passphrase on the console. No secrets are stored unencrypted anywhere other than server / application memory.

Infrastructure and Facilities

AWS operates the cloud infrastructure that Cureatr uses to provision a variety of basic computing resources such as processing and storage. The AWS infrastructure includes the facilities, network, and hardware as well as some operational software (e.g., host OS, virtualization software, etc.) that supports the provisioning and use of these resources.

The AWS infrastructure is designed and managed according to security best practices as well as a variety of security compliance standards. Further details on the following areas can be found at:

- https://aws.amazon.com/whitepapers/
- https://aws.amazon.com/security/security-resources/
- https://aws.amazon.com/compliance/resources/

- AWS Overview
- AWS Compliance – SOC1,2,3, HIPAA
- Physical Security – Perimeter, Facility access, Video Surveillance
- Environmental Security
- Network Security
- AWS Account Security
- Business Continuity and Disaster Recovery

On top of the AWS infrastructure, Cureatr manages all security and compliance aspects we are responsible for, such as OS patch management, vulnerability management, network security management, etc.

High-Availability Architecture

Cureatr follows the recommended AWS best practices for building scalable and highly available applications.

- Cureatr system is spans multiple Availability Zones, which is the basic element of AWS redundancy architecture. More information can be found at http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html
- Every externally available core service is backed by multiple servers in 2 or more availability zones, fronted by Elastic Load Balancers that route traffic away from any instances that become unavailable to service requests
- AWS makes it trivial to launch new instances to augment existing ones or replace ones that fail. Cureatr manages infrastructure as code, which means it's trivial to provision new instances configured with the required services and applications.
- For storage, Cureatr utilizes a mix of databases managed in highly-available clustered configurations, and AWS-supported highly available storage services (RDS, Redshift, S3)
- Virtually every internal service is designed with the expectation that individual components can and will fail. We utilize queuing extensively to ensure guaranteed processing of critical tasks.

- Cureatr AWS infrastructure is configured to have redundant network paths in and out of the environment for all network-dependent services.
- All systems and applications are fully monitored with internal and external monitoring. Critical failure alerts are delivered to the operations team in real-time.
- Finally, Cureatr software development and release processes are optimized for 100% target uptime. We can and have performed very complex updates and total migrations of our infrastructure without incurring any scheduled downtime.

Summary

Cureatr is a secure, scalable, and highly-available application. Our approach protects the confidentiality of our customers' data and information in a highly secure and compliant manner, whether the data resides within the application, on device being used, in transit, or inside our server infrastructure.