Security Program Overview

Table of Contents

Intended Audience:

This document was created by ELB Learning for potential and existing CenarioVR customers. The information it contains explains the way in which CenarioVR handles customer data, along with the overall technical architecture of the platform. The document addresses topics related to the CenarioVR architecture and the provision of CenarioVR cloud services. The intended audience for this document is: stakeholders from Risk Management, IT Engineering, Project Officers, Senior Consultants or Project Sponsors.

1.0 Architecture Overview

CenarioVR is software developed by ELB Learning. It relies on the following back-end stack for its functionality:

Linux - The main operation system for the servers
Nginx - The web server
Amazon RDS - A cloud database from Amazon
Java - The programming language in which the application is written

The application also leverages the Spring framework for Java development.

The software is operated in a multitenant architecture that is designed to segregate and restrict customer data access based on business needs. The architecture provides an effective logical data separation for different customers via customer-specific "Organization IDs" and allows the use of customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production.

PC: Author/Viewer Front-End

CenarioVR requires a modern web browser that supports JavaScript, and does not require any third party plugins. It currently supports the following browsers:

- Chrome
- Mozilla Firefox
- Microsoft Edge
- Safari 10 or above

These browsers are supported on the following operating systems:

- Microsoft Windows 7 and above
- OSX

In all instances, ELB Learning strongly recommends that clients maintain updated operating systems aligned to the latest release made available by the respective vendors.

Mobile: Viewer Front-End

CenarioVR supports viewing scenarios in the browser of mobile devices. CenarioVR follows the Responsive Web Design approach, allowing for optimal viewing across a wide range of devices.

Mobile Operating Systems:

- iOS - Default browser in iOS version 10 and above
- Android - Chrome browser in Android 8 and above

CenarioVR also has dedicated apps for both iOS and Android, available on the respective stores for each platform. These apps are the preferred method of delivery for mobile, as they download all content to the device before playing, eliminating any buffering of streaming content. They also enable automatic update of content on the device when it is published from the CenarioVR authoring platform.

Headsets: Viewer Front-End

CenarioVR also has native Apps for the following headset platforms:

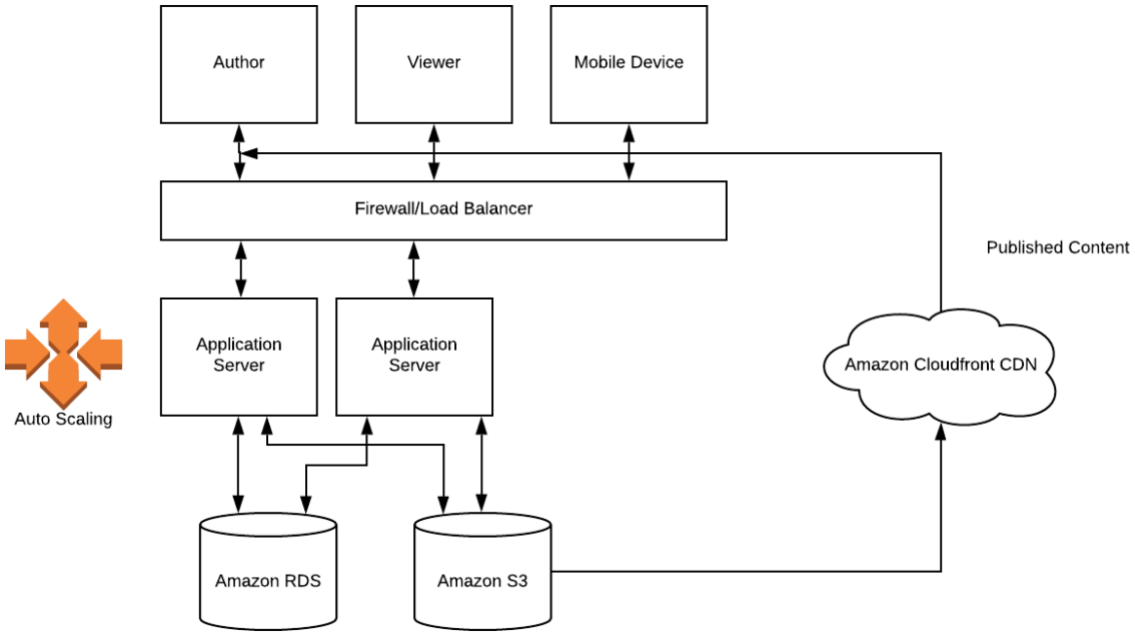
- Samsung Gear VR
- Oculus Go
- Oculus Quest
- Oculus Rift/Rift S
- HTC Vive Focus
- HTC Vive/Pro
- Pico Neo/G2/G2 4K

These apps work in the same manner as the iOS and Android apps in that they download the content locally to the device before running the content, and manage content updates from the CenarioVR authoring platform.

1.1 Platform Architecture

The CenarioVR architecture is designed to be fault tolerant and auto healing. The diagram below describes this architecture in greater detail.

Architecture Diagram:



Application servers are automatically spun up or down as needed through Amazon Elastic Beanstalk in the Amazon US East-1 Region. Instances can be started in any of the 6 availability zones in the region for fault tolerance. New code deployments are managed by injecting new application servers into the system, and deprecating the existing servers, ensuring a smooth rollout of new versions.

The Amazon RDS database is used to store users, settings, assignments, and references to user generated content. All user generated content is stored inside the secured Amazon S3 object storage and delivered via the Amazon Cloudfront CDN, ensuring rapid delivery of content worldwide.

1.2 Content Delivery

CenarioVR uses the Amazon Cloudfront CDN. This CDN is a globally distributed network of servers that can replicate the static contents to a location (edge location) that is as close as

possible to the final user's location. This helps reduce latency and increase the speed of content navigation, as well as drastically increasing the concurrent supported users.

The list of available edge locations, as of August 2019 is:

North America	**Europe**	**Asia**
Ashburn, VA	Amsterdam	Bangalore, India
Atlanta, GA	The Netherlands	Chennai, India
Boston, MA	Berlin, Germany	Hong Kong, China
Chicago, IL	Copenhagen, Denmark	Hyderabad, India
Dallas/Fort Worth, TX	Dublin, Ireland	Kuala Lumpur, Malaysia
Denver, CO	Frankfurt, Germany	Mumbai, India
Hayward, CA	Helsinki, Finland	Manila, Philippines
Hillsboro, OR	London, England	New Delhi, India
Houston, TX	Madrid, Spain	Osaka, Japan
Jacksonville, FL	Manchester, England	Seoul, South Korea
Los Angeles, CA	Marseille, France	Singapore
Miami, FL	Milan, Italy	Taipei, Taiwan
Minneapolis, MN	Munich, Germany	Tokyo, Japan
Montreal, QC	Oslo, Norway	
New York, NY	Palermo, Italy	**Australia**
Newark, NJ	Paris, France	Melbourne
Palo Alto, CA	Prague, Czech Republic	Perth
Philadelphia, PA	Stockholm, Sweden	Sydney
Phoenix, AZ	Vienna, Austria	
Salt Lake City, Utah	Warsaw, Poland	**Africa**
San Jose, CA	Zurich, Switzerland	Johannesburg, South Africa
Seattle, WA		Cape Town, South Africa
South Bend, IN	**Middle East**	
Toronto, ON	Dubai, United Arab Emirates	**China**
	Fujairah, United Arab Emirates	Beijing
South America	Tel Aviv, Israel	Shanghai
São Paulo, Brazil		Zhongwei
Rio de Janeiro, Brazil		

For the latest updated list, please refer to:
http://aws.amazon.com/cloudfront/details/#Detailed_Description

2.0 Scalability and Redundancy

The main factors that allow CenarioVR to achieve scalability and redundancy is the physical and logical separation between the application engine and user-generated content, and the stateless mode in which the application runs. These allow CenarioVR to serve the user's request from multiple web servers instead of a single server.

This achieves redundancy (reliability) by replicating more than one backend through different servers. Each backend has the ability to resolve a user’s request. This means that if a server fails to respond, another healthy instance can be reached while the unhealthy server recovers. Scalability is a direct application of the same logic. When a high load of traffic is detected, new backend servers are automatically added that can resolve a user’s request and properly manage the increase in traffic.

3.0 Backup Policies

3.1 Database Backup Policies

An entire database backup is performed daily. Daily data is retained on a 14 day rotating cycle.

3.2 User Retention Policies

Trial user data is backed up and stored for 30 days after a trial has ended. If a user signs up within 30 days after the trial, they still will retain all content created during the trial period. Client data is preserved for 90 days after termination of a user's account.

3.3 User Generated Content

User generated Content is stored on the Amazon S3 storage technology. The structure of S3 storage automatically keeps multiple copies of the same object in different Amazon servers for business continuity purposes and in order to ensure a 99.999999999% data durability.

4.0 Disaster Recovery and Business continuity

4.1 Business continuity

CenarioVR leverages Elastic Beanstalk to automatically rebuild instances in another availability zone in the unlikely instance of the failure in any availability zone. Each availability zone is designed as an independent failure zone. The database is mirrored between two availability

zones, providing a high level of resilience to failure. Recovery from an availability zone failure should be a matter of minutes.

4.2 Disaster Recovery

In the case of a major disaster, recreation of the CenarioVR service will be done in another availability zone. In general, this can be done in a matter of hours using images and backup data held in Amazon S3.

5.0 Password Restriction Policies

CenarioVR allows administrators to configure different levels of complexity in password management, depending on their housekeeping and internal security policies. Some of the password-related capabilities from an LMS administrator's standpoint are to:

- Set minimum length (default 6)
- require the use of both upper-case and lower-case letters (default off)
- inclusion of one or more numerical digits (default off)
- prohibition of words found in a password blacklist (default off)
- prohibition of words found in the user's personal information (default off)

All passwords are stored using a highly secured (encrypted hash), non-reversible algorithm. ELB Learning staff are, therefore, unable to retrieve a previously stored password by any user in the system/database. However, users can use the password recovery functionality to be guided into setting up a new password.

6.0 Sessions

User sessions are maintained inside a central database repository. The association between a session and the user assigned to that session is performed via a session token only. This solution, in conjunction with the use of a secure connection with https, prevents the possibility of session hijacking.

Sessions are checked for unique logged-in users. If two separate sessions are identified simultaneously by the same username, the first one will be logged out from the System.

7.0 Content Encryption

Content encryption over the network between the client and CenarioVR servers is achieved through the use of HTTPS. All connections to the server are forced to be via HTTPS.

8.0 SQL Injections

An SQL Injection is a hacking technique that targets applications that use SQL databases. It tries to inject malicious code into SQL queries in order to retrieve extra information or to change some of the application's behavior.

In order to prevent SQL injection, the application uses Spring Data JPA/Hibernate with bound parameters, and dynamic queries provided by the framework. This eliminates the possibility of a SQL injection.

9.0 Cross-site Request Forgery

CSRF attacks use URLs generated from outside our application with the aim of getting them to perform unwanted operations.

To prevent CSRF attacks, CenarioVR uses JWT tokens for authentication. Tokens are passed via a header parameter so that the browser can't automatically authenticate the requests, therefore making CSRF impossible.

10.0 Vulnerability Detection

The CenarioVR servers are scanned monthly using Nessus by Tenable, the most accurate and comprehensive vulnerability assessment solution in the market. The Nessus software scans for more than 45,000 Common Vulnerabilities and Exposures (CVE), with new plugins released weekly, or within 24 hours of a vulnerability disclosure.

11.0 Audits and Certifications

As ELB Learning understands that security and reliability are critical elements in the choice of a Cloud-based software solution, it maintains high security standards and, in line with such standards, carefully selects its providers by partnering with those organizations that not only prove the highest industry ratings in their specific services but also ensure the highest level of reliability and security.

Amazon Web Services (AWS), the world's leader in Cloud and CDN provisioning for software vendors, is continuously audited, with certifications from accreditation bodies across geographies and verticals, including ISO 27001, FedRAMP, DoD CSM, and PCI DSS. The

following link provides extensive information and data related to risk management and risk prevention associated due diligence:

https://aws.amazon.com/security/
http://aws.amazon.com/compliance/