e2m.live

the event app co.

POWERED AT NYC

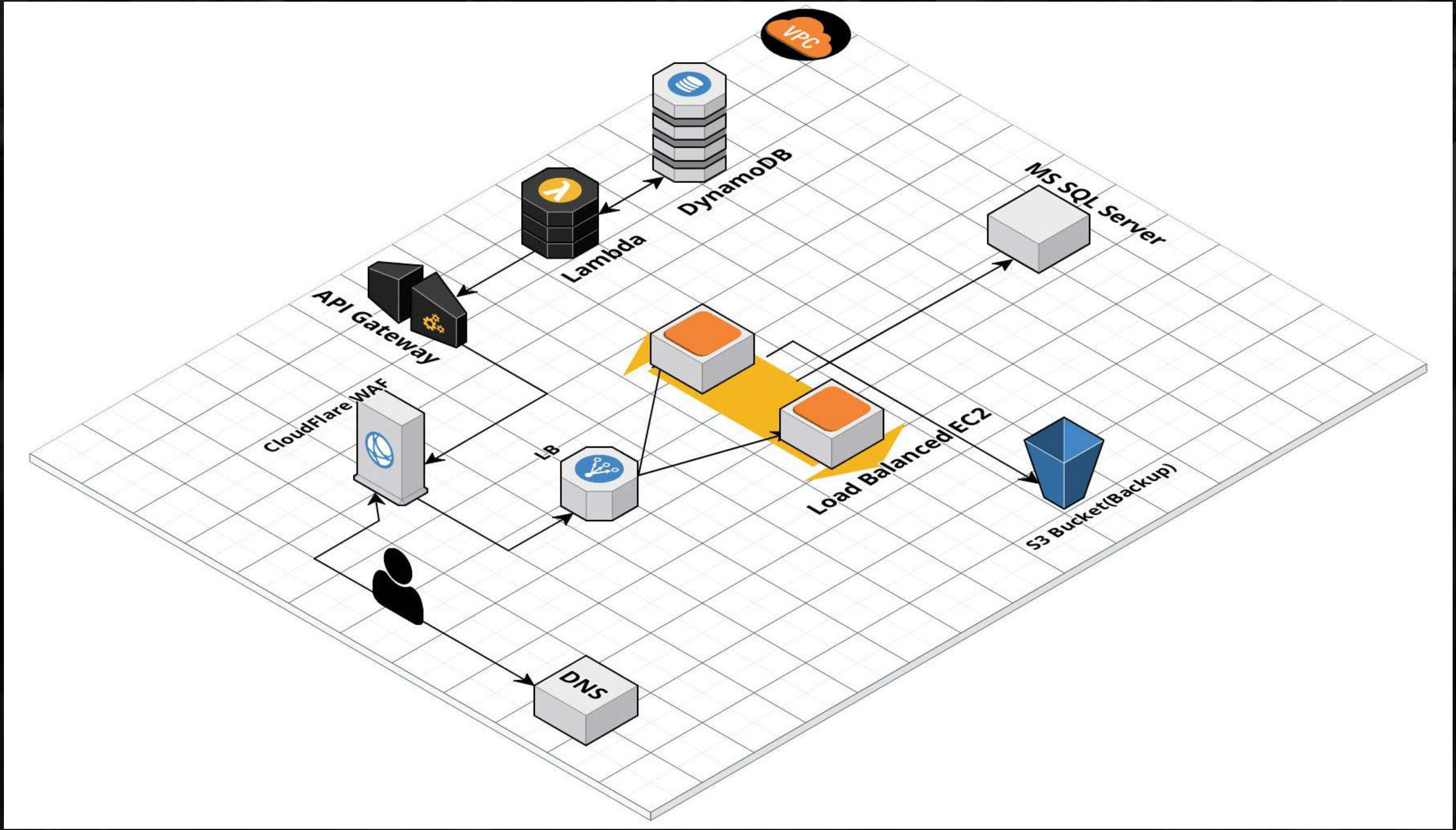
Innovate, engage & connect with e2m

SECURE EVENT APP

www.e2m.live

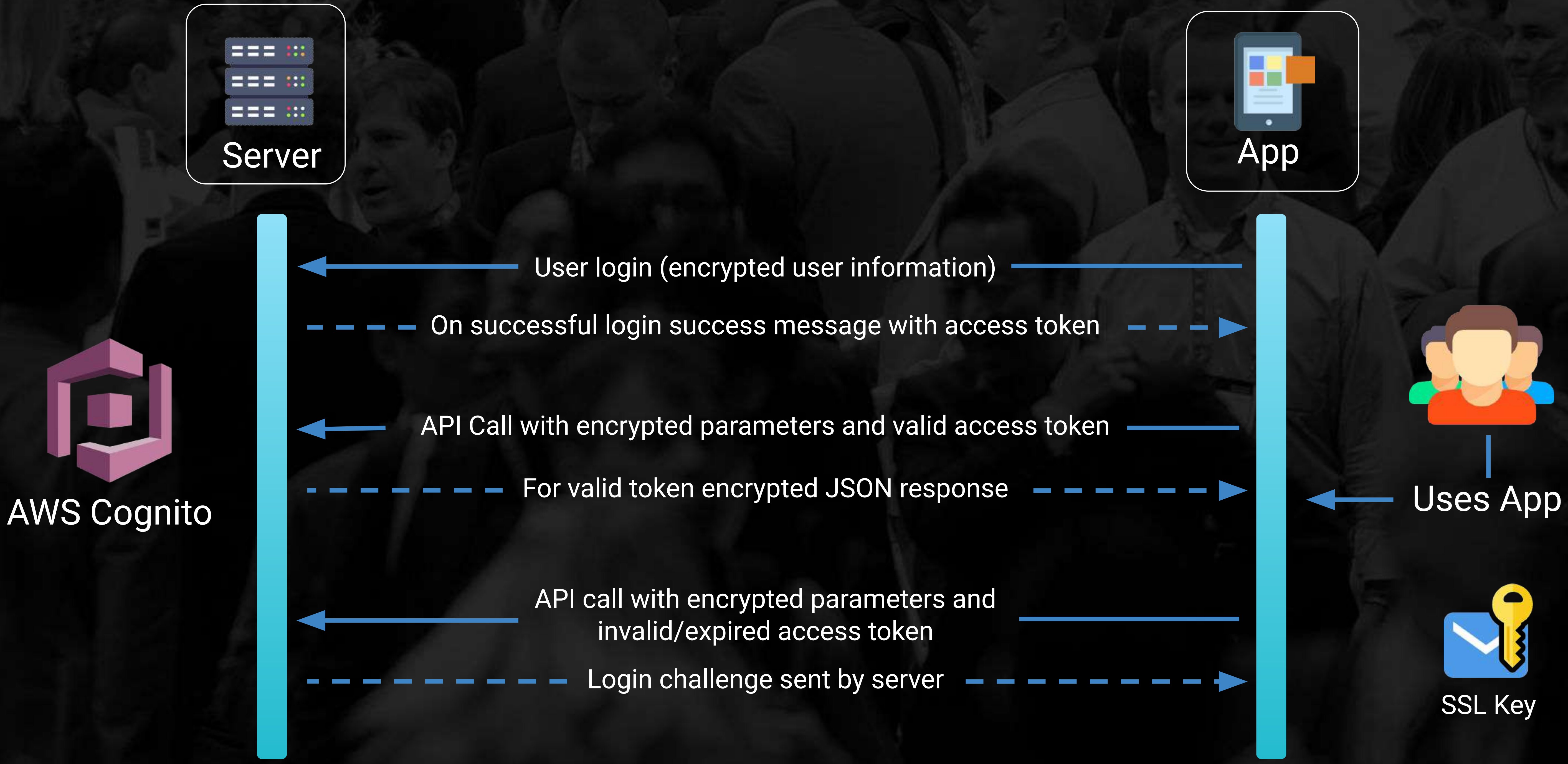
Infrastructure & Security

AWS Infrastructure



e2m.live
the event app co.

User Authentication Process



Server

App

User login (encrypted user information)

On successful login success message with access token

API Call with encrypted parameters and valid access token

For valid token encrypted JSON response

API call with encrypted parameters and invalid/expired access token

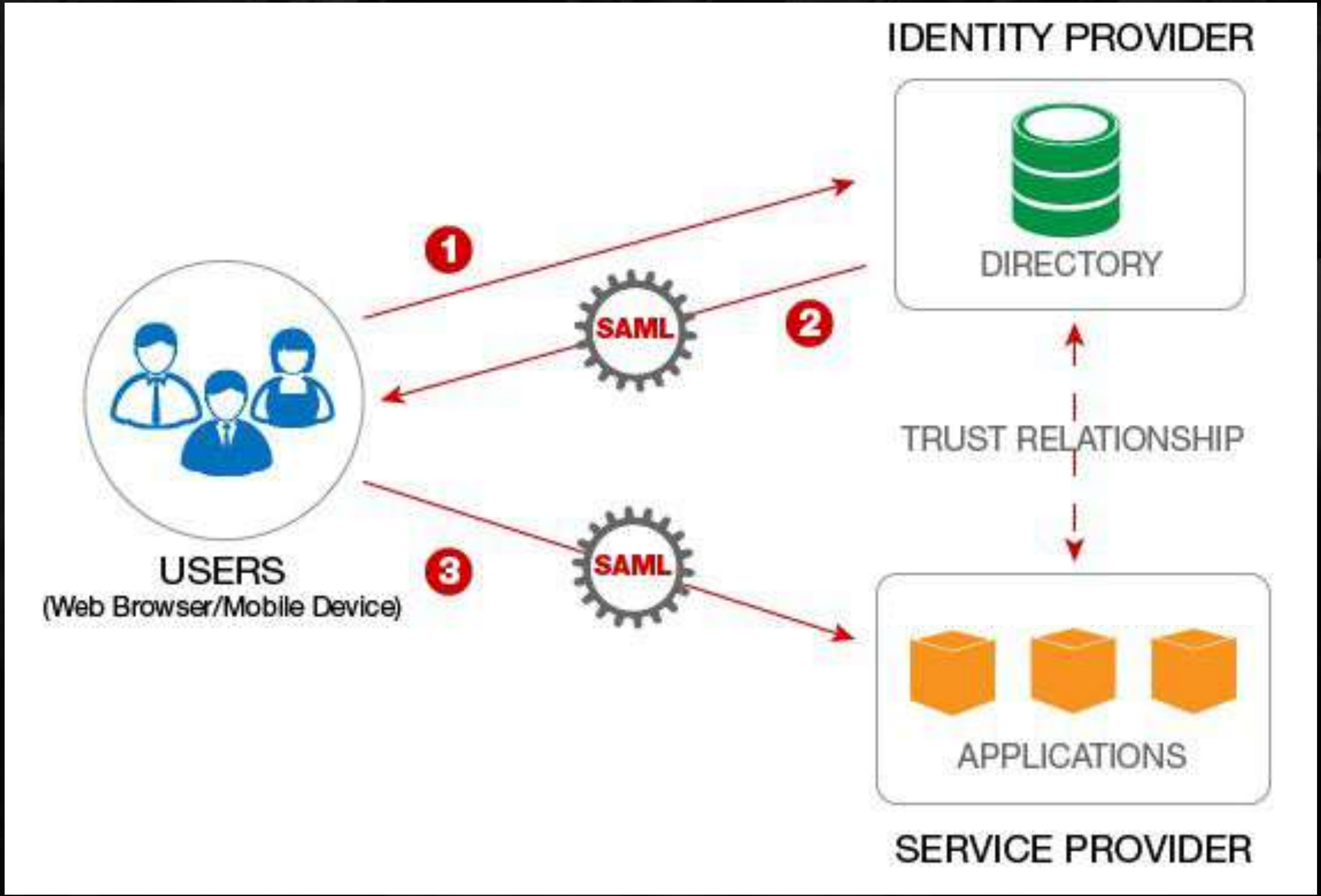
Login challenge sent by server

AWS Cognito

Uses App

SSL Key

SSO Support



okta

f5

Azure Active Directory

and more...

e2m.live
the event app co.

Web & Mobile Security Testing

acunetix

Developer Report

Acunetix Security Audit

02 May 2019

Generated by Acunetix

Confidential

Oct. 24, 2019, 3:31 a.m. UTC

App Security Report

For Internal Purpose

Web Spiders Group

Events

co[redacted]

4.9.8

Prepared by

appknox

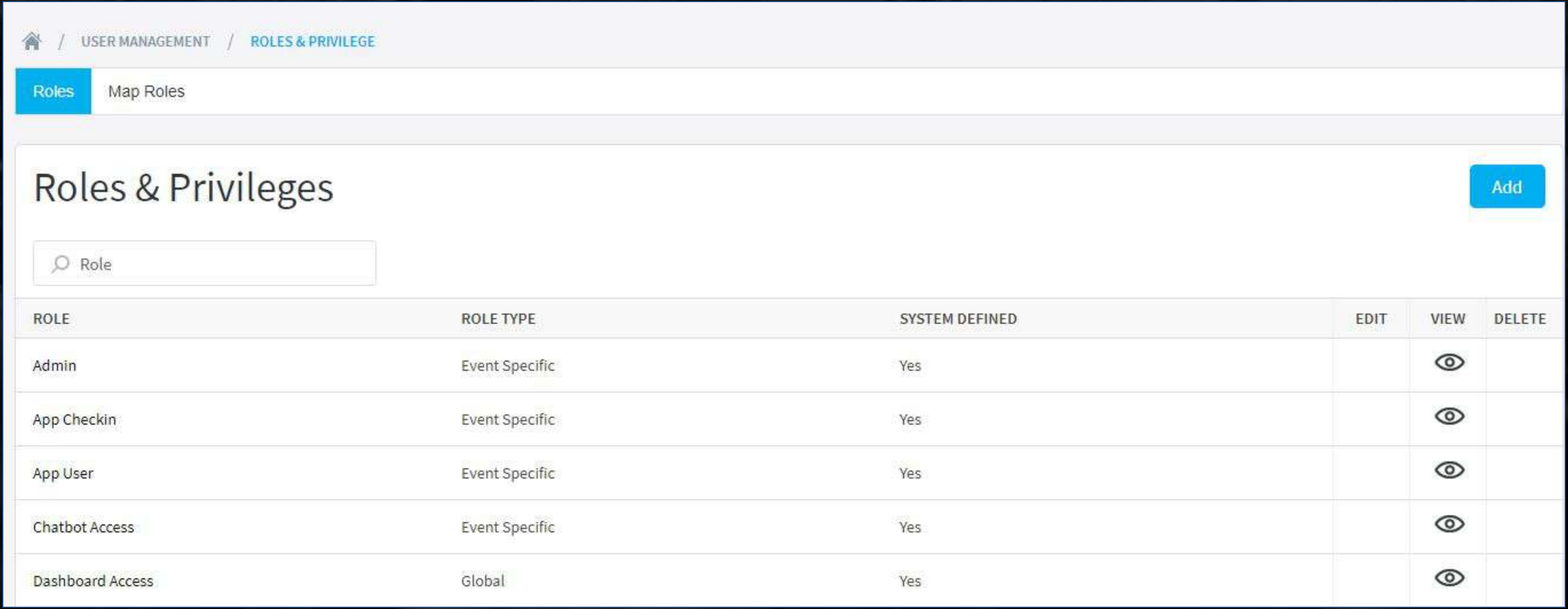
Portions of this document and the templates used in its production are the property of Appknox and cannot be copied without permission.

While precautions have been taken in the preparation of this document, the publisher and the author(s) assume no responsibility for errors, omissions, or for damages resulting from the use of the information contained herein. Use of Appknox services does not guarantee the security of a system, or that intrusions will not occur.

Page 1 of 41

Secured Privilege based access to CMS and App

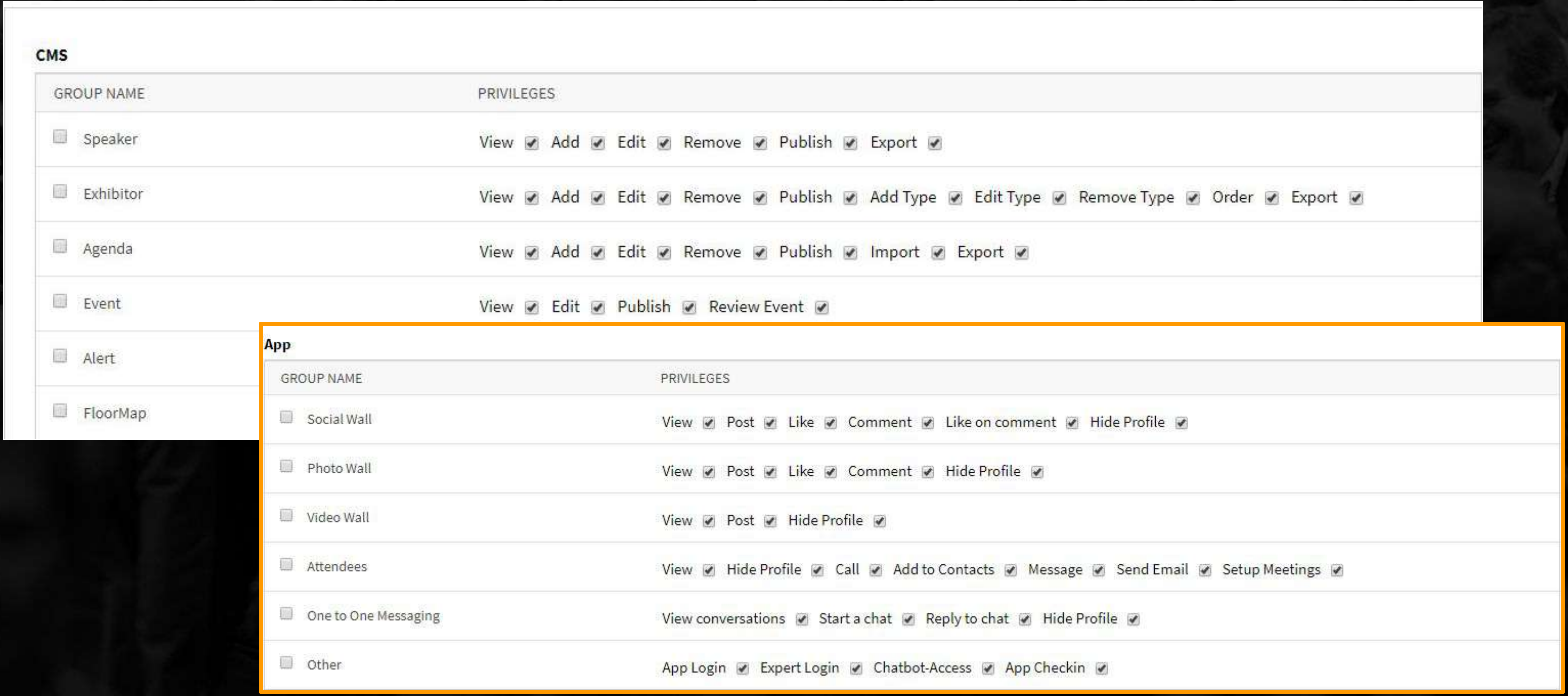
e2m.live
the event app co.



Roles & Privileges

ROLE	ROLE TYPE	SYSTEM DEFINED	EDIT	VIEW	DELETE
Admin	Event Specific	Yes		👁	
App Checkin	Event Specific	Yes		👁	
App User	Event Specific	Yes		👁	
Chatbot Access	Event Specific	Yes		👁	
Dashboard Access	Global	Yes		👁	

Mapping User Roles to Privileges



CMS

GROUP NAME	PRIVILEGES
□ Speaker	View ☑ Add ☑ Edit ☑ Remove ☑ Publish ☑ Export ☑
□ Exhibitor	View ☑ Add ☑ Edit ☑ Remove ☑ Publish ☑ Add Type ☑ Edit Type ☑ Remove Type ☑ Order ☑ Export ☑
□ Agenda	View ☑ Add ☑ Edit ☑ Remove ☑ Publish ☑ Import ☑ Export ☑
□ Event	View ☑ Edit ☑ Publish ☑ Review Event ☑
□ Alert	
□ FloorMap	

App

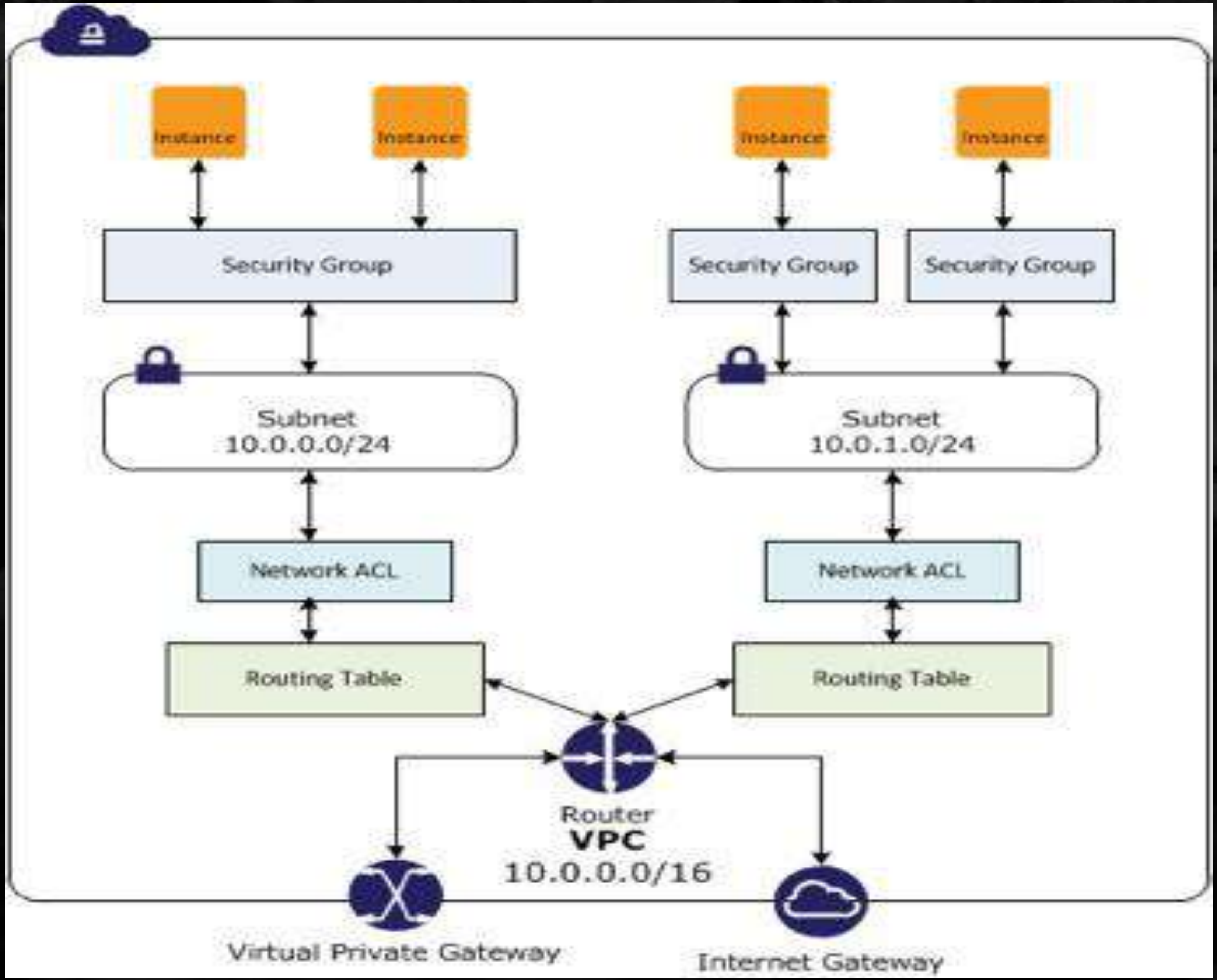
GROUP NAME	PRIVILEGES
□ Social Wall	View ☑ Post ☑ Like ☑ Comment ☑ Like on comment ☑ Hide Profile ☑
□ Photo Wall	View ☑ Post ☑ Like ☑ Comment ☑ Hide Profile ☑
□ Video Wall	View ☑ Post ☑ Hide Profile ☑
□ Attendees	View ☑ Hide Profile ☑ Call ☑ Add to Contacts ☑ Message ☑ Send Email ☑ Setup Meetings ☑
□ One to One Messaging	View conversations ☑ Start a chat ☑ Reply to chat ☑ Hide Profile ☑
□ Other	App Login ☑ Expert Login ☑ Chatbot-Access ☑ App Checkin ☑

Hosting & Scalability

E2M backend systems are hosted on Amazon AWS EC2 dedicated instances within VPC environment

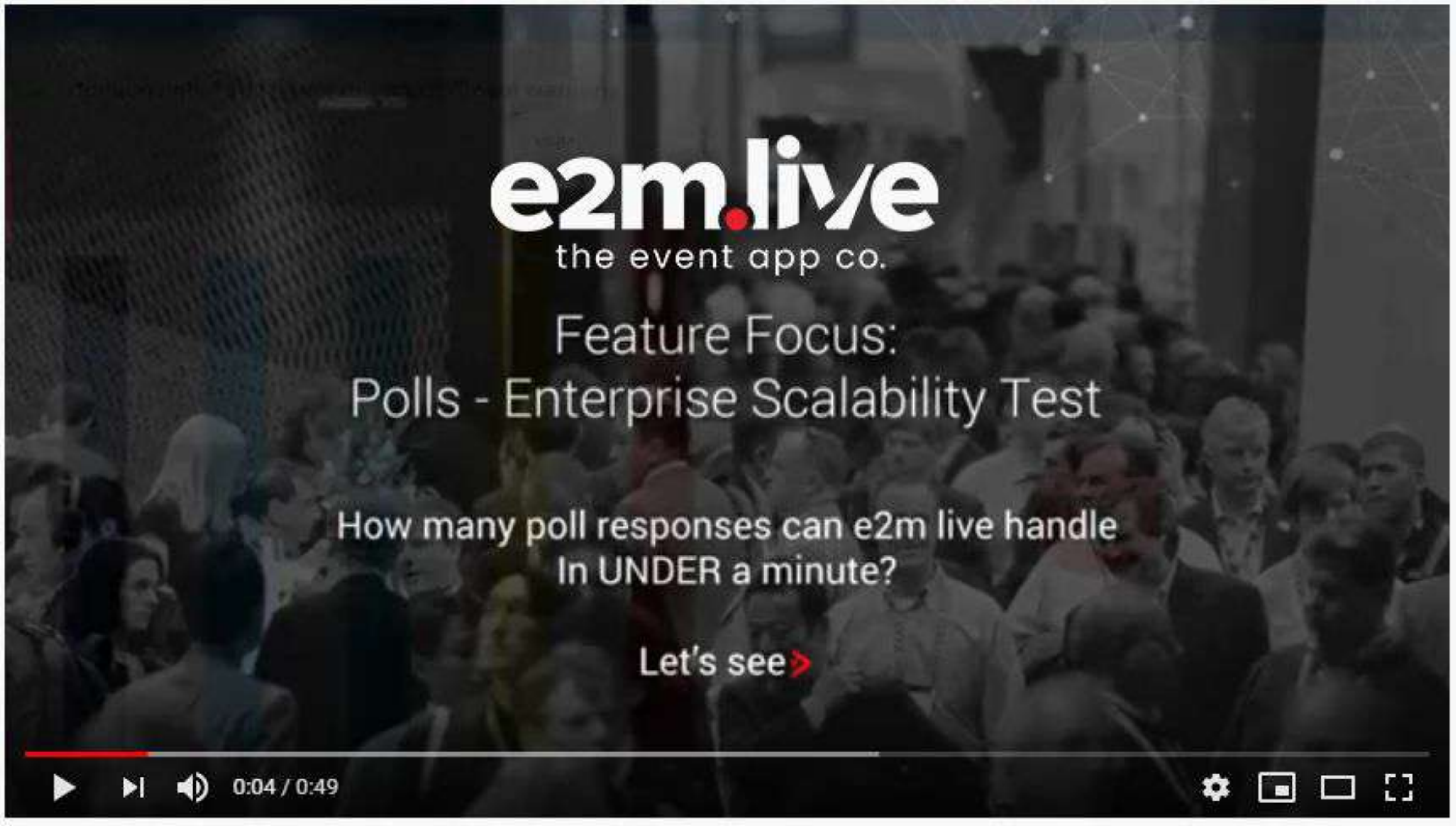
VPC design & cloud strengthening

e2m.live
the event app co.



IAM aws

e2m.live
the event app co.



e2m.live
the event app co.

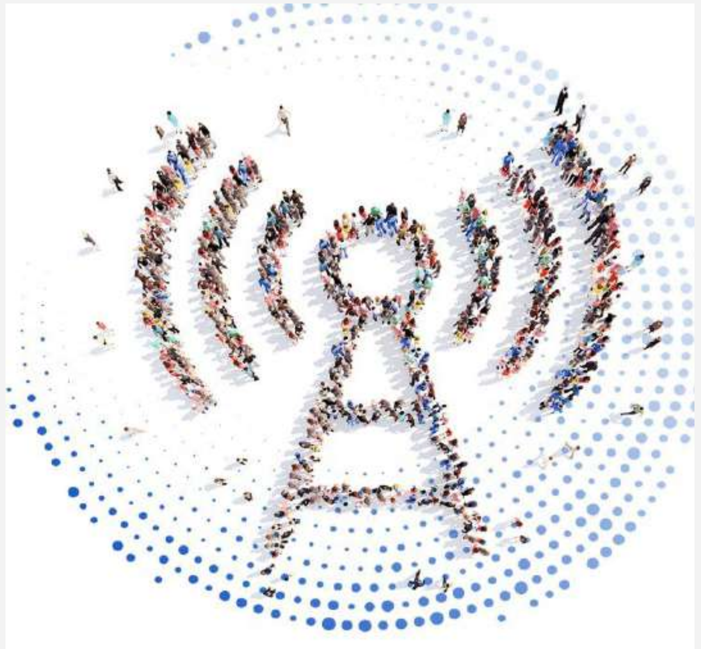
Feature Focus:
Polls - Enterprise Scalability Test

How many poll responses can e2m live handle
In UNDER a minute?

Let's see

Real-time Communication framework

Scalable Sub-Second Low Latency Anywhere in the World. Powered by Agora's SD-RTN™ - the world's most widely used and intelligent RTC network.



Intelligent RTC network, dedicated to extreme low latency, high availability real-time voice, and video within and across borders. **99.995% uptime**

Scale with Confidence. Supports over 200,000 peak concurrent users (CU) in a single broadcast channel.

Security - Video Audio & Broadcast

Data Encryption
The Agora channel is encrypted with the AES-128 or AES-256 algorithm between clients and the client/server.

Conversation Content
Media contents are encrypted on the end devices, and the Agora Cloud does not have any key to decrypt them.

End User Data
All end-user level data such as logins, identities, and personal information.
This data is not shared with Agora.

e2m.live
the event app co.

Thank You

PROPOSED IT/NETWORK INFRASTRUCTURE

TYPE	PERFORMANCE FEATURES
Web Servers	Load Balanced Autoscale mode handles failover, server scaling and performance
Database Servers	Separation of Read Replica Server and Main Server ensures performance, and scalability. Multi AZ will ensure redundancy in Main and Read Replica.
Application Servers	Load Balanced Autoscale mode handles failover, server scaling and performance
Cloudflare CDN	CDN for faster content delivery and WAF(Web Application Firewall) for protection from DDOS and SQL Injection.
REDIS, MEMCACHE	Caching mechanisms to improve performance
API Gateway	Better API Management
Firebase Notifications	No need to poll server periodically for status updates, reduces load on server

e2m.live
the event app co.

Data Security

#	Data protection	Details	
1.	*Encryption: data at rest*	*On the Server:*	***All sensitive data elements at rest are stored in secure RDBMS system protected with integrated Windows authentication and physical file access control via Windows ACL.***
		On the Device:	Custom instrumentation has been implemented to encrypt and decrypt sensitive data stored locally on the device using strong encryption algorithm like **[AES 256-bit]**.
2.	*Encryption: data in transit*	***Encryption of data in transit has been implemented by using TLS (HTTPS) in all communications between the backend server system and mobile devices or desktop browsers.***	
3.	Remote wipe (In case MDM is used)	The system enables remote wipe of the sensitive data stored in the device in case it is lost or stolen.	
4.	*File security*	***Sensitive data stored locally on device or in the backend server.*** ***Strong encryption algorithm like [AES 256-bit] has been used***	

Data Security

5.	256 bit encryption	• For data-at-rest: Strong encryption algorithm like [AES 256- bit] has been used for the custom encryption of sensitive data-at-rest on mobile devices. • For data-in-transit: 256 bit encryption has been implemented for data-in-transit by procuring and installing
6.	*Application data and/or service access*	• ***Both of the CMS and the Service systems implements UserID and Password based authentication to prevent unauthenticated access of data and services.*** • ***The application implements role based access priviledge to protect unauthorised access of data and services.*** • ***JWT token Authorization has been implemented at the webservice layer to prevent unauthorized access on both Apps and Mobile web.***

Data Security

Topic	Description
Data at rest	*On the Server: Data at rest on the server will be protected with the help of disk level encryption offered by AWS EC2.*
Data in transit	Encryption of data in transit will be implemented by using TLS (HTTPS) in all communications between the backend server system and mobile devices or desktop

E2M Hosting

E2M backend systems are hosted on **AWS EC2** dedicated instances within VPC environment

Secure access – Customer access points, also called API endpoints, allow secure HTTP access (HTTPS) so that you can establish secure communication sessions with your AWS services using SSL/TLS 1.2.

Built-in firewalls – E2M can control how accessible our instances are by configuring built-in firewall rules – from totally public to completely private, or somewhere in between. And when our instances reside within a Virtual Private Cloud (VPC) subnet, we can control egress as well as ingress.

Unique users – The AWS Identity and Access Management (IAM) tool allows us to control the level of access our own users have to our AWS infrastructure services. With AWS IAM, each user can have unique security credentials, eliminating the need for shared passwords or keys and allowing the security best practices of role separation and least privilege.

Multi-factor authentication (MFA) – AWS provides built-in support for multi-factor authentication (MFA) for use with your root AWS Account as well as individual IAM user accounts under it.

Private Subnets – The AWS Virtual Private Cloud (VPC) service allows you to add another layer of network security to your instances by creating private subnets and even adding an IPsec VPN tunnel between your home network and your AWS VPC.

Encrypted data storage – Customers can have the data and objects they store in Amazon EBS, Amazon S3, Glacier, Redshift, and Oracle and SQL Server RDS encrypted automatically using Advanced Encryption Standard (AES) 256, a secure symmetric-key encryption standard using 256-bit encryption keys.