eventmobi

Security, reliability, disaster recovery, and compliance

Last updated: January 2023

Security

Physical Security of Servers

Amazon manages EventMobi servers through their extensive Amazon Web Services (AWS). AWS data centers are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication no fewer than three times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

Amazon only provides data center access and information to employees who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical and electronic access to data centers by Amazon employees is logged and audited routinely.

For further details see https://aws.amazon.com/security/

As part of our Internal Policies, only Engineers who have met our employment checks (see Internal Policies section) and probationary period receive access to the Amazon Web Services Portal. Two-factor authentication is required and by default engineers are given least-privilege access.

Amazon Web Services Data Processing Addendum

EventMobi has signed a copy of the Amazon Web Services Data Processing Addendum.

For more information, please visit: https://aws.amazon.com/compliance/eu-data-protection/

Physical Security of EventMobi Office / Contents

EventMobi employees agree to security and privacy policies to manage and keep safe confidential data on their laptops, phones, and other electronic devices. Equipment is regularly audited to ensure that specified policy is in place. Employee card access is required at all times to gain access to the office building. Our office internal wifi networks are secured using WPA2-PSK passcodes.

We leverage the power of Cisco's Meraki MDM agent on all our devices to produce a hardware policy and to inventory all our IT assets. We regularly audit for non-compliant devices and remediate them personally and immediately including keeping the Operating System patches and Anti-Virus definitions up-to-date.

All EventMobi employee computers have their hard drives encrypted using the AES-XTS mode of AES with 128 bit blocks and a 256 bit key to encrypt the disk. Computers are forced to be locked within a short time span and are forced to have password protection on wake-up.

USB keys are prohibited from being taken out of the office and any data storage devices (NAS) are physically secured from removal.

Third party applications used by EventMobi employees are only accessible via the single sign-on identity provider OneLogin. This ensures we have appropriate access control for data in those applications. In order to access OneLogin, employees must have a sufficiently strong password which is rotated every 6 months and use two-factor authentication.

Login Protection

All passwords for user and organizer accounts are hashed using the bcrypt one-way hashing algorithm, with a salt. Passwords are required for all event app users.

Encryption

All communication between your devices and EventMobi's platform and APIs are fully protected by Secure Socket Layer Encryption (SSL) to protect your data from man-in-the-middle attacks and eavesdropping. SSL certificates are provided by GeoTrust and GlobalSign.

EventMobi leverages built-in encryption in Amazon Web Services' RDS service which enables the at-rest encryption of data in the database (and all backups) using the industry standard AES-256 cipher. The keys are generated by and protected by a Hardware Security Module provided by Amazon Web Services.

GeoTrust® GlobalSign® GMO INTERNET GROUP

Vulnerability Assessments and Penetration Testing

To safeguard our internal systems, EventMobi performs routine scans of our servers for known vulnerabilities.

At least once per year and when enough of the codebase has changed, EventMobi retains a third party firm to perform a vulnerability assessment on our products.

Customers who wish to perform a penetration test of their own will need to fill out and return a copy of the Penetration Test Request Form.

Data Privacy and Protection Policies

Data Processing & Data Control

We encourage customers to enter into our standard Data Processing Addendum (DPA) that outlines the roles and responsibilities both EventMobi (as Data Processor) and the event planner (as Data Controller) have with regard to personal data collection, storage and usage in the course of their use of the EventMobi platform.

We have validated our own data security and processing policies, and documented processes for responding to data access requests, including the provision of data (under the right to access) and destruction or anonymization of data (under the right to be forgotten) when directed to do so by a Data Controller (the organization planning the event).

We offer customers the ability to publish a Privacy Notice and Terms Of Use to participants of their event and provide model language for each.

Reliability & Disaster Recovery

Redundant Servers and Data Centers

EventMobi's architecture is designed to be redundant and fault tolerant. We are committed to providing and maintaining a highly available system. That being said, it is nearly impossible to account for all possible failure incidents and interruptions and thus we have built safeguards for these cases.

EventMobi uses Amazon AWS services as its primary hosting platform. For information on our infrastructure-level protections, see https://aws.amazon.com/security/ for details taken by our hosting partner (Amazon) for security, availability, and recovery. We make use of EC2 server instances (see http://aws.amazon.com/ec2-sla/ for EC2 SLA), host our database on RDS services, replicated for fail-over protection, and S3 buckets for eleven 9s (99.999999999%) of data durability.

Database Backups

The data in your EventMobi account is replicated across multiple database servers to prevent a single database failure from causing data loss.

Additionally, that data is backed up every 20 minutes and stored securely using Amazon's geographically-distributed and fault tolerant S3service. This ensures that in the event of a catastrophic failure within the data center, your information will be safe and your records can be restored within a short amount of time.

We maintain all backups for a period of at least 7 days in an encrypted state and restore the latest backup daily to ensure it will work if needed in an incident scenario.

User Uploaded Data Reliability

Any user-uploaded data (including images, documents, and videos) is uploaded to the Amazon S3 platform (see http://aws.amazon.com/s3-sla/ for S3 SLA), which is designed to achieve 'eleven 9s' (99.999999999%) of data durability, 99.99% availability and is automatically replicated across multiple data centers.

Service Restoration

EventMobi has invested in and built cloud computing and deployment automation tools to streamline our day to day operations. This automation is crucial to our disaster recovery plan as every deployment we perform is the same process required to restore service from a service disruption where restoration from backups is required. Our application deployments occur on a daily basis and thus our automated tools are regularly checked and confirmed to be functional.

Our architecture allows us to build a disaster recovery plan that can sustain failure across datacenters in Amazon Web Services's Virginia region. We have servers running across at least 3 of those datacenters and are able to use our existing automation to deploy to all 5.

Downtime monitoring and performance notifications

Our recovery plan is built upon enterprise level notification and monitoring systems. We use Pagerduty, a geographically distributed monitoring service to perform uptime and performance checks on our systems on a 60-second granularity. Should any alerts arise, our engineering team is alerted by mobile push notification, email, or phone call and will follow a clearly defined protocol to handle the event.

pagerduty

Customer Communication

Communication and customer service are always our top focus at EventMobi. Should any service interruption occur, oursupport team will proactively reach out to affected parties via email or phone and keep them up-to-date regarding the situation. Open communication and insight into these problems is key to maintaining the trust of our clients.

Incident Post-Mortem

Within 24 hours of any service interruption, our support team will follow up with you to explain the root cause of the issuealong with how we have remedied it and how we will prevent this in the future.

Scalability

EventMobi's systems are robust and set up to scale to meet customer demands. We have an auto-scaling capability thatwill provision and deploy additional servers to handle excess load. This, however, requires certain load thresholds to be met and ~10-15 minutes is required for new servers to be provisioned and configured for use. It is possible to experience performance issues. Even though this will be rare, we keep a pre-provisioned server on hot-standby.

To preempt these issues, simply let us know of your large scale use plans, and we will provision extra servers on the day of your event to prepare for large scale usage.

Internal Policies

EventMobi internal policies are based on the Cloud Security Alliance Consensus Assessment Initiative questionnaire(CAIQ).

cloud security alliance

More information is available at: https://cloudsecurityalliance.org/group/consensus-assessments/. All EventMobi employees and contractors sign NDA regarding custom data they interact with, and further EventMobi performs criminal and background checks on any hire coming into the company. We regularly create and distribute training material on security best practices and how to properly deal with customer data, sensitive or otherwise.

Product development at EventMobi follows the OWASP Secure Software Development Life Cycle ensuring Security Engineers are brought in as early as possible for the creation of a feature to help our engineers ensure our products are designed and remain secure.

Reporting & Audit Trails

EventMobi gathers and collects comprehensive audit trails for all activity performed on the EventMobi systems. Logs produced by Amazon Web Services are centrally stored in Amazon Web Services CloudTrail and CloudWatch. Logs produced by EventMobi systems are centrally stored in Splunk and kept 90 days. Admins can track account actions, username, email addresses, IP addresses along with date/time for all actions.

Responsible Disclosure

EventMobi is committed to integrating security best practices into every aspect of development. We do not currently participate in a bug bounty program, but take privacy and vulnerabilities very seriously. If a member of your organization finds any security issues, please contact security@eventmobi.com.

Privacy Policy & Terms Of Use

EventMobi's Privacy Policy can be found at http://www.eventmobi.com/privacy-policy/

EventMobi's Terms of Use can be found at http://www.eventmobi.com/terms-of-use/