Yapp Security

Yapp Overview

Yapp provides a mobile and cloud application platform used by organizations of all sizes to create, distribute and maintain mobile apps for events, teams and groups around the world. Our platform provides an extremely fast and easy creation process that does not require that our customers have technical expertise. This frees them to focus on their business goals while Yapp focuses on mobile SDKs, API performance, scaling, security and more. Yapp applies security best practices across the product and we are able to quickly deploy security updates without customer interaction or service interruption.

Security Assessments and Compliance

Data Centers

Yapp's server infrastructure is hosted on Amazon Web Services (AWS) and physically resides within Amazon's secure data centers. Amazon continually manages risk and undergoes recurring assessments to ensure compliance with industry standards. Amazon's data center operations have been accredited under:

- ISO 27001
- SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
- PCI Level 1
- FISMA Moderate
- Sarbanes-Oxley (SOX)

PCI

We use PCI-compliant payment processor Stripe for encrypting and processing credit card payments. Stripe is certified to PCI Service Provider Level 1, the most stringent level of certification available. Our server infrastructure at AWS is also PCI Level 1 compliant. Credit card numbers are never made available to Yapp's servers and Stripe stores card numbers encrypted on disk with AES-256 per their PCI compliance.

SSL and HTTPS

Yapp forces HTTPS for all API communications as well as for our public website, protecting Yapp end users from packet sniffing and man-in-the middle attacks.

Mobile Data Storage

Yapp maintains applications installable from the iOS App Store and Google Play Store. These "container" applications contain the totality of executable code allowed by Yapp apps and allow downloads of the customer-facing apps, which are stored on the mobile devices in directories designated for access by the Yapp application only.

Images and Documents

Image and document uploads are managed by and orchestrating secure storage on AWS S3. Files are stored using UUID-based file paths and all file transport occurs over SSL. Image delivery is accomplished in conjunction with imgix, a vendor providing on-demand resizing, cropping, and caching of images. End users may save image and documents to their device. Yapp does not endorse distributing highly-sensitive documents via apps created on our platform.

Live-updating data

In order to provide real-time updates to end users for certain categories of dynamic data including social posts, comments, reactions, and photo uploads, Yapp sends updates via a secure web socket connection maintained by the mobile device clients. The websocket connection, authentication, and routing tasks are performed by Pusher, a vendor specializing in such functionality. All communication with Pusher and end-user devices is channel-based and occurs via SSL. Per-channel security is authenticated at connection time using Yapp's API.

Physical Security

Yapp utilizes ISO 27001 and FISMA certified data centers managed by Amazon. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. 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 additional information see: https://aws.amazon.com/security

Environmental Safeguards

Fire Detection and Suppression

Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Power

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide backup power for the entire facility.

Climate and Temperature Control

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Monitoring systems and data center personnel ensure temperature and humidity are at the appropriate levels.

Management

Data center staff monitor electrical, mechanical and life support systems and equipment so issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

For additional information see: https://aws.amazon.com/security

Network Security

Firewalls

Yapp utilizes hosting platform services from Heroku, a Salesforce company, which manages firewalls on our behalf. Firewalls are utilized to restrict access to systems from external networks and between systems internally. By default all access is denied and only explicitly allowed ports and protocols are allowed based on business need. Each system is assigned to a firewall security group based on the system's function. Security groups restrict access to only the ports and protocols required for a system's specific function to mitigate risk.

Host-based firewalls restrict other AWS or Heroku cloud customers from establishing localhost connections over the loopback network interface to further isolate Yapp's APIs from any other applications.

DDoS Mitigation

Heroku provides Yapp with DDoS (Distributed Denial of Service) mitigation techniques including TCP Syn cookies and connection rate limiting in addition to maintaining multiple backbone connections and internal bandwidth capacity that exceeds the Internet carrier supplied bandwidth.

Spoofing and Sniffing Protections

Managed firewalls prevent IP, MAC, and ARP spoofing on the network and between virtual hosts to ensure spoofing is not possible. Packet sniffing is prevented by infrastructure including the hypervisor which will not deliver traffic to an interface which it is not addressed to.

Port Scanning

Port scanning is prohibited and every reported instance is investigated by our infrastructure providers. When port scans are detected, they are stopped and access is blocked.

Data Security

Postgres Databases

Yapp customer data is stored in Postgresql database instances managed by Heroku. Each database requires a unique username and password that is only valid for that specific database and is unique to Yapp. Connections to our postgres databases require SSL encryption to ensure a high level of security and privacy.

No PCI-impacting data is stored in this database instance.

Password Storage

Passwords in a salted and hashed form. Salting and hashing is performed using bcrypt, which also allows us to increase iteration count over time to make the key derivation slower and resistant to brute-force search attacks even as computation power increases. Yapp's APIs implement protections against timing-based password attacks as well.

System Security

System Configuration

System configuration and consistency is maintained through standard, up-to-date images, configuration management software, and by replacing systems with updated deployments. Systems are deployed using up-to-date images that are updated with configuration changes and security updates before deployment. Once deployed, existing systems are decommissioned and replaced with up-to-date systems.

System Authentication

Operating system access is off limits even to Yapp staff. Application console and administrative access is limited to employees with business needs and requires authentication.

Backups

Postgres Databases

Via Heroku Postgres, Yapp utilizes Continuous Protection as an ongoing backup/recovery mechanism. Every change to customer data is written to write-ahead logs, which are shipped to multi-datacenter, high-durability storage. In the unlikely event of unrecoverable hardware failure, these logs can be automatically 'replayed' to recover the database to within seconds of its last known state. Yapp also performs automated nightly backups and retain the last 7 days as well as weekly snapshots going one month back. Data backups are stored securely at AWS S3 and accessible only with signed, expiring URLs that can be generated only by Yapp staff with necessary access privileges.

Disaster Recovery

Yapp leverages Heroku's platform to automatically restore Yapp services and data in the case of an AWS outage. The Heroku platform dynamically monitors for failures and recovers failed platform components.

Yapp Architecture

The Yapp platform is designed for stability and scaling, and inherently mitigates common issues that lead to outages by eliminating any manual server-specific configuration.

Customer Data Retention and Destruction

When Yapp customers remove data from the platform, it is immediately removed from API-accessible database storage, and will be retained in backups for 1 month pursuant to the Backups section above.

Decommissioning hardware is managed by AWS using a process designed to prevent customer data exposure. AWS uses techniques outlined in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data.

Privacy

Yapp has a published privacy policy that clearly defines what data is collected and how it is used. Yapp values customer privacy and transparency. We takes steps to protect the privacy of our customers and protect data stored within the platform. For additional information see https://www.yapp.us/u/privacy

Access to Customer Data

Yapp staff does not access or interact with customer data or applications for day-to-day operational purposes. There may be cases where Yapp needs to interact with customer data or applications for customer support purposes or where required by law.

Limiting Your App's Distribution and Use

Yapp's platform provides three options for controlling who can access each app you create on the platform. First, you may allow anyone with the install link (https://my.yapp.us/[YOUR_YAPP_ID]) to install the app. This is the least secure but allows your end users to remain anonymous, which is important for some customers. Second, you

may whitelist your end users by email and require that they have proved control of an allowed email address before they can install your app. You may revoke access from any of these users at any time, and your app will be removed from their phone. Finally, you may require that end users be authenticated with any confirmed email address in order to access your app. This option also allows revoking access and ensures that all app activity can be linked back to a specific email address.