488 Bryant Street, San Francisco, CA 94107
envoy.com | (415) 636-6605

Our company

Envoy is a company backed by industry leaders like Andressen Horowtiz, Adam D'Angelo (ex-CTO of Facebook), Marc Benioff (CEO of Salesforce), Jeremy Stoppelman (CEO of Yelp), Alexis Ohanian (Chairman of Reddit), Garry Tan/Harj Taggar (Partners at YCombinator), and many others. Having raised over $15M, we have grown our team, become cash flow positive, and we're here to stay and build the product for the long term.

Envoy operates in hundreds of companies across every continent of the world (except Antartica). Our customers range from private companies like Airbnb, Box, Evernote, and Shopify; public companies like Yelp, Pandora and Tesla; government contractors like Planet Labs; hospitals like The Children's Hospital of Philadelphia and schools such as Children's Day School and Alt School in San Francisco, Cranmer Primary School in London, and Ohio State University. Many of our customers, like Uber, take advantage of Envoy in multiple countries and securely manage them all from one central office.

We're here to stay. Our product focused approach is how we've built the best product out there and why it'll continue to be the best going forward. The progress we've made in the past year and a half is indicative of the progress we'll make the next. Envoy is the safe bet when deciding on who to use not just today and tomorrow, but ten years from now.

Reliability

- In the highly unlikely event of a server outage, all data is kept on the iPad and retried until successfully stored with us. We have never lost a customer's data.
- The iPad will also fully function in offline mode.
- All data is stored in an encrypted form either in Heroku Postgres or encrypted Amazon S3 Buckets. Data is continuously versioned for recovery purposes.
- We provide a transparent status page so you always know about outages and service availability.

Envoy Employee Access

We have strict policies that Envoy employees should only be accessing production data when debugging a problem that's only reproducible in production.

We log everything that can be accessed in production:

- Database queries
- Console access and commands ran on production
- Deploys and who committed what code
- HTTP requests on our admin pages and other pages
- All data is stored as write-only into S3 for infinite access
- All code in production is peer reviewed by at least one other engineer

Employees are required to use dual-factor passwords whenever a service we use has the ability, and use full-disk encryption and screensaver lock in 2 minutes or less. Authentication to SSH is always done via private key and not password.

We have policies that require employees to never store production data on their laptops. Employees are required to use strong passwords and the 1Password software to ensure a unique password for every service they use.

488 Bryant Street, San Francisco, CA 94107
envoy.com | (415) 636-6605

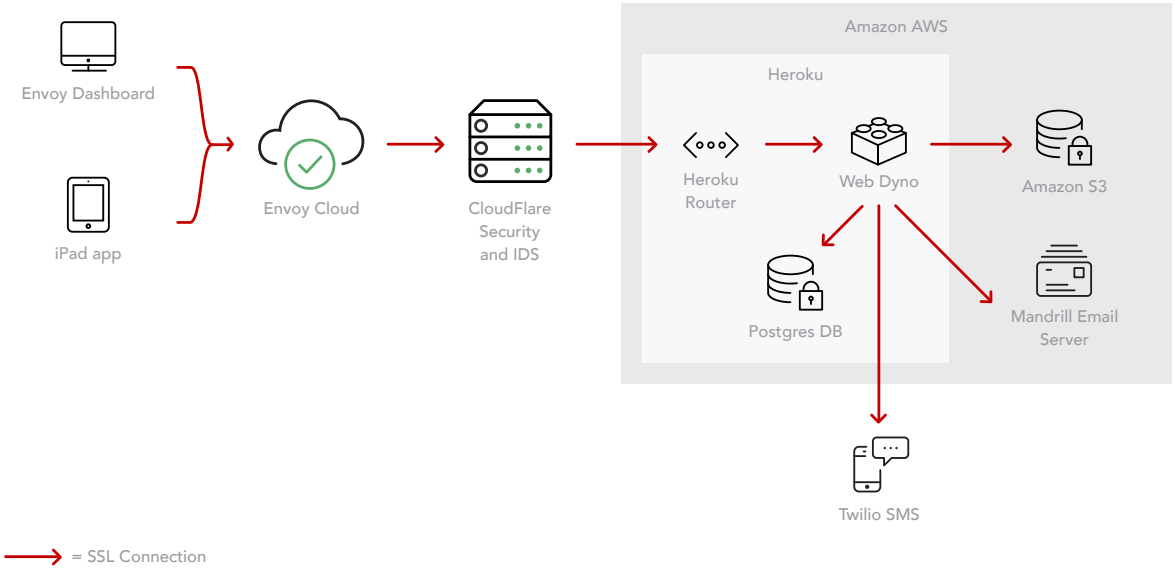
Encryption

- At the transport layer, all data is encrypted
  - TLS from the iPad to Cloudflare
  - TLS from Cloudflare to Heroku
  - Encrypted Postgres session to the Postgres database
  - Encrypted REST calls to Amazon S3 for accessing
  - Webhook and API both are encrypted
  - Certificates are always checked on *both* sides

- At the steady-state, data is also encrypted.
  - We are on the encrypted Postgres database tier on Heroku
  - We use Amazon S3 encrypted buckets

- Our website is only accessible via HTTPS. We do not give you the option of accidentally using regular HTTP for browsing pages. Logged-in or not.

Envoy Network Architecture



Security Precautions

- We do not host any servers ourselves. It is outsourced to professionals like Heroku and Amazon.
- Cloudflare is used for all network requests. Cloudflare provides an IDS on incoming traffic. For more information.
- Amazon security policies. We host assets such as signed NDAs and visitor photos on S3.
- Heroku security policies. We host sign-in metadata on Heroku and encrypted Heroku Postgres.
- Both Amazon and Heroku, though multi-tenant, have strict controls to prevent one tenant from accessing the data of another.
- SAML support such that you don't need to share usernames/passwords.
- Security desk url and visitor pre-registration pages have randomly generated URLs and are unguessable. In the event of this url being compromised, you can always re-generate it.
- We always use the latest technologies at the latest patch levels.
- Due to enforced ActiveRecord scoping in our source code, it is impossible for one authenticated user to access the data of another.
- Of course, all passwords are hashed and salted. You can only reset a password, not retrieve it. Additionally, all parties are notified when the email address for a user has been changed.
- We do not store your credit card information in any database, you directly communicate with Stripe, which is PCI compliant when storing your information.
- All URLs which link to S3 include tokens to always expire after 1 hour. This prevents the scenario where an admin might accidentally leak a CSV of all photos/NDAs.
- As your data is stored on our servers, you are not vulnerable to a burglar taking your log in book or servers from your physical premises.
- We always test for SQL Injection and verify the authenticity of POST, PUT and DELETE requests to prevent CSRF attacks.
- We rate limit all aspects of our website, everything from log in attempts, password reset attempts, etc.
- We whitelist attributes on all models to prevent mass-assignment vulnerabilities.
- Application credentials are kept separate from the database and codebase.

Great for providing security to your business

- ITAR requires you know if people in your building are US residents or not. Envoy's custom fields allow for you to figure this out by asking the visitor.
- Many financial regulations require you keep an active list of everyone who had access to your building for auditing purposes.
- Many municipalities require you know who is in the building in the event of a fire/emergency.

We keep only the data that's necessary to run our service

- For employee notification if you want to only send us emails or only phone numbers or only the first letter of the last name, we don't require anything else from you.
- When importing from your LDAP or AD, we let you push data to us as opposed to you being required to open ports for us to go in to get data.
- You can delete entries at any point. Deletes are permanent and cannot be restored. Same goes for location or account deletions.

Privacy-aware

- Envoy is Safe-Harbor certified for handling visitor information throughout Europe. This means we believe in the privacy rights of visitors and upon request will delete a person's information upon request. Before deletion, we will provide the current visitor history logs to the company in order to maintain their records.
- When visitors self-sign-out, we do not display a list of people that are signed in. You must know 3 letters of someone that's actually signed in to see the full name.
- When visitors select employees, again, you must know 3 letters of their name. We never display your full employee directory to a visitor
- When a recurring visitor identifies via email, we hide their restored phone number. Same when identifying via phone, we hide email.

Penetration testing

- Although we haven't had any penetration testing by an official firm that specializes in it, we have had lots of independent pen testing by firms like: Yahoo, Pandora, Palantir, and many others.
- We are also publicly listed on HackerOne. A community where hackers compete to pen-test products for points and bounties. So far we have had no major problems. Our servers are being attacked 24/7 and we live in an environment of constant penetration testing. See our page here.
- You are welcome to audit our source code or get a firm to audit us. All we ask is that you let us know when it will happen, plus in source code scenarios we'd like to be present as it happens.