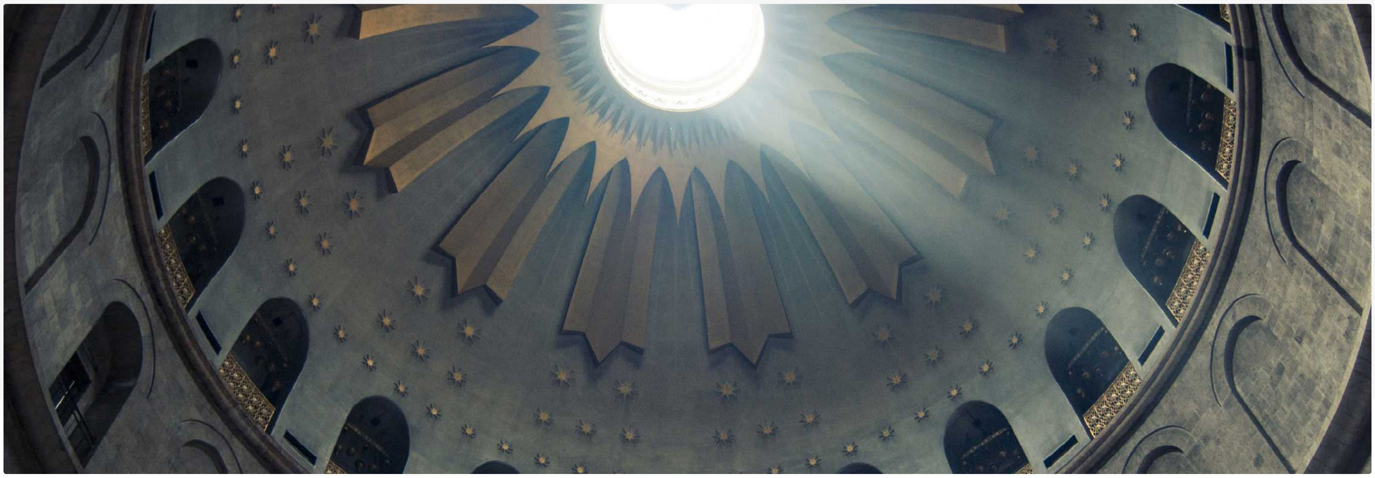


Security and privacy

At Envoy, we understand the sensitivity of your data

At Envoy, we understand the sensitivity of your data, and we're committed to ensuring confidentiality and reliability as critical components of our service to you. We take your trust very seriously, and we're proud to provide a secure infrastructure that protects your visitor data and company information.

> **"Since Envoy's first day, when I was the engineer building our initial product, security has always been a first-class citizen. Our customers' trust is critical, and we realized this early on. Even with Envoy's expanding functionality, data security is still key and is part of every decision we make. That's how it always will be."**
>
> —Larry Gadea, CEO of Envoy

Thousands of global companies choose and trust Envoy, from private companies like Pixar and Reddit, to public companies such as Yelp, Pandora, Box and Shopify. Plus, customers from highly-regulated industries like OnRamp (data center), Roche (pharmaceutical) and Planet Labs (government) all depend on Envoy to demonstrate compliance.

Reliability

We understand the importance of reliability and aspire to a 99.9% uptime. We continually monitor uptime through third parties like Pingdom. You can view our current uptime and product status by visiting status.envoy.com.

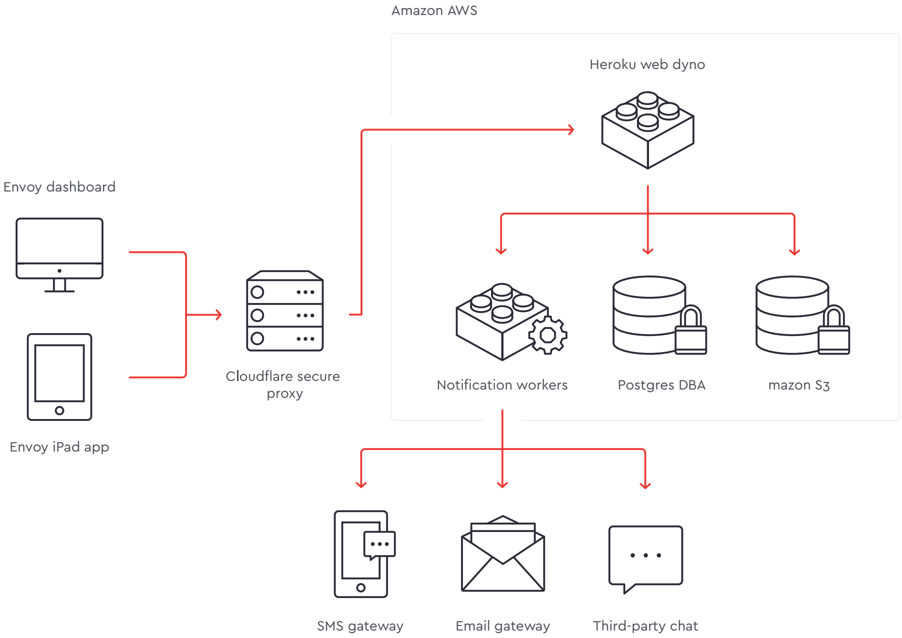
Data storage

When your iPad is connected to a network, visitor data syncs to Envoy automatically, and all visitor records are stored in Envoy's database. Backups are taken every day and stored offsite in the AWS US-West-2 data center in Oregon. Envoy never stores customer data on local devices or any other internal network.

Centralized account management

Envoy makes it easy to centrally manage data and permissions for multiple facilities, no matter where you're located. Role-based administration allows customers to provide the right Envoy access to specified team members on global or location-specific levels. And SAML can be utilized to integrate with your single sign-on identity provider to further regulate access.

All visitor information is stored in secure cloud servers and can only be accessed by specified administrators. Robust visitor logs can be exported with just one click, an especially useful feature for our customers that require compliance with PCI, DSS, ITAR and other frameworks.



Secure and trusted infrastructure

All customer data is transferred securely using HTTPS (SSL connection) from the iPad app and Envoy dashboard to secure cloud and servers. At rest, data is encrypted using Heroku encrypted databases and AWS S3 Server-side Encryption. Envoy protects against denial-of-service (DoS) attacks using CloudFlare's advanced DDoS protection.

Offline-mode

If devices become disconnected from a network connection, visitors can continue to sign in on the iPad, and their data will be stored locally on the device. Upon reestablishing network connectivity, all locally stored visitor data will sync to Envoy.

Privacy

We have a strict policy to respect the privacy of sensitive customer data: we will never sell your visitor or employee data, and we will not contact your visitors or employees without explicit permission. Our support team will only access your account in the event of a technical support issue that requires real-time access.