Envoy

Protecting your data and privacy

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.

Keeping your data secure

Data encryption

All customer data is transferred securely using TLS v1.2 and above from the iPad app and Envoy dashboard to the cloud. All requests are routed through Cloudflare which acts as a firewall. At rest, data is encrypted using AWS for databases and Cloudflare for object storage. Both AWS and Cloudflare use AES256 for disk encryption. Our IT infrastructure is 100% cloud-based.

Data storage

When your iPad or mobile device is connected to a network, data syncs to Envoy automatically, and all records are stored in Envoy's database. Backups are taken every day and stored off-site in either the AWS US-East-1 data center in Virginia, US-West-1 data center in California, or US-West-2 data center in Oregon. AWS oversees the physical security of these facilities and tightly controls who has access.

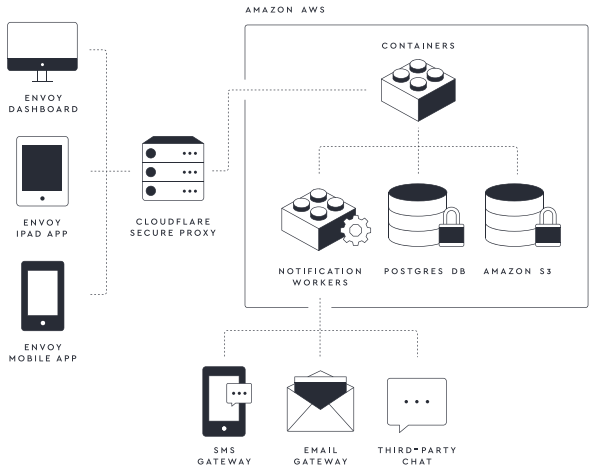
Data retention

Customers can choose to retain or purge the responses to their visitor and employee sign-in questions. Purged responses are sent to Envoy's server to determine if that person is approved or denied entry, which occurs in sub-seconds. The data is then immediately queued for deletion. We run periodic jobs to ensure all data, except for the screening result, is deleted within 24 hours on all of Envoy's databases.

Additional visitor and employee data, such as name and arrival time, can be purged upon explicit request. Data can be anonymized, which removes all personally identifiable information from your Visitor Log, upon request. Data is available for download as a CSV file through the dashboard or via our API. Envoy may retain customer data for up to 30 days after the termination of the contract.

Verified security practices

Our security processes and controls are verified to meet SOC 2 Type II security standards. This includes using two-factor authentication, encrypting computers, logging administrator actions, tracking access grants using verified policies, and following repeatable processes for a consistent and secure customer experience.



Envoy

Reliability and offline-mode

We understand the importance of reliability and aspire to a 99.9% uptime. Envoy proactively protects against denial-of-service (DoS) attacks using CloudFlare's advanced distributed DoS protection. We continually monitor uptime through third parties like Pingdom. You can view our current uptime and product status by visiting status.envoy.com.

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. While offline, ID scanning and host notifications will be unavailable.

Security testing

We seek out and proactively address vulnerabilities and exposures in Envoy's code and dependencies through automated tools, peer-review, penetration tests, and a public bug bounty program. All public access to our applications is proxied through Cloudflare which detects and automatically blocks unexpected traffic.

Protecting privacy

Privacy policy

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.

Employee and visitor privacy

If you choose to ask questions about your employees' or visitors' health, you can choose to discard their responses and keep them private to those individuals. If you choose to discard responses, your team will not have access to this data in any form, whether through a dashboard, report, or otherwise. To help your team keep your workplace safe, administrators can see if someone was approved or denied entry based on their responses.

Access 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.

Compliant with standards and regulations

We have made significant efforts to ensure we are in compliance with the General Data Protection Regulation (GDPR) and to help our customers comply with GDPR contractual obligations. To enter into Envoy's Data Processing Addendum (DPA), please contact security@envoy.com to receive a copy for review and signature.