Mio

Security White Paper

Mio is making cross platform communication between teams a reality. In doing so, protecting the integrity and security of your data is of paramount importance to us. This is why Mio never stores your messages or your files. This document presents our transparent approach to security so your company can have a high degree of confidence when communicating over our systems. Our SOC-2 Type II audit report is available upon request.

Service Organization Control (SOC) 2 Type II

Mio is SOC-2 Type II certified to keep customer data secure and confidential.

General Data Protection Regulation (GDPR)

Mio adheres to GDPR guidelines to protect our customers' personal data and privacy rights.

California Consumer Privacy Act (CCPA)

Mio has implemented controls from the CCPA framework to support our customers' rights over their personal data.

Security by design

It is our philosophy that security should be incorporated into our product design from day one. All projects we undertake are subject to a risk assessment to ensure we don't compromise our underlying security policies. Mio is SOC 2 Type II certified and is committed to keeping your data secure.

Organizational security

We educate our team through mandatory security training to understand the importance of keeping your user data secure, which includes enforcing industry standard authentication and authorization methods as well as maintaining the privacy of the personal information you transmit over our network.

Classifying and prioritizing data

We classify and prioritize data to ensure we can provide the highest possible tier of security to your online messaging transactions. If we can avoid persistent or temporary storage of your data we will do so, and if we need to retain sensitive or critical data we will encrypt it and ensure it can be destroyed at the earliest possible opportunity.

Protecting your data

Data encryption in transit and at rest

All data that is transmitted via Mio systems uses the TLS 1.2 or later, and sensitive payloads are encrypted using AES-256 or equivalent ciphers. We connect to external messaging partners using the strongest grade encryption protocols they support and will proactively upgrade when new standards become available. Data at rest is encrypted to a minimum AES-256 standard at the vendor layer with additional controls applied at the application level for sensitive data.

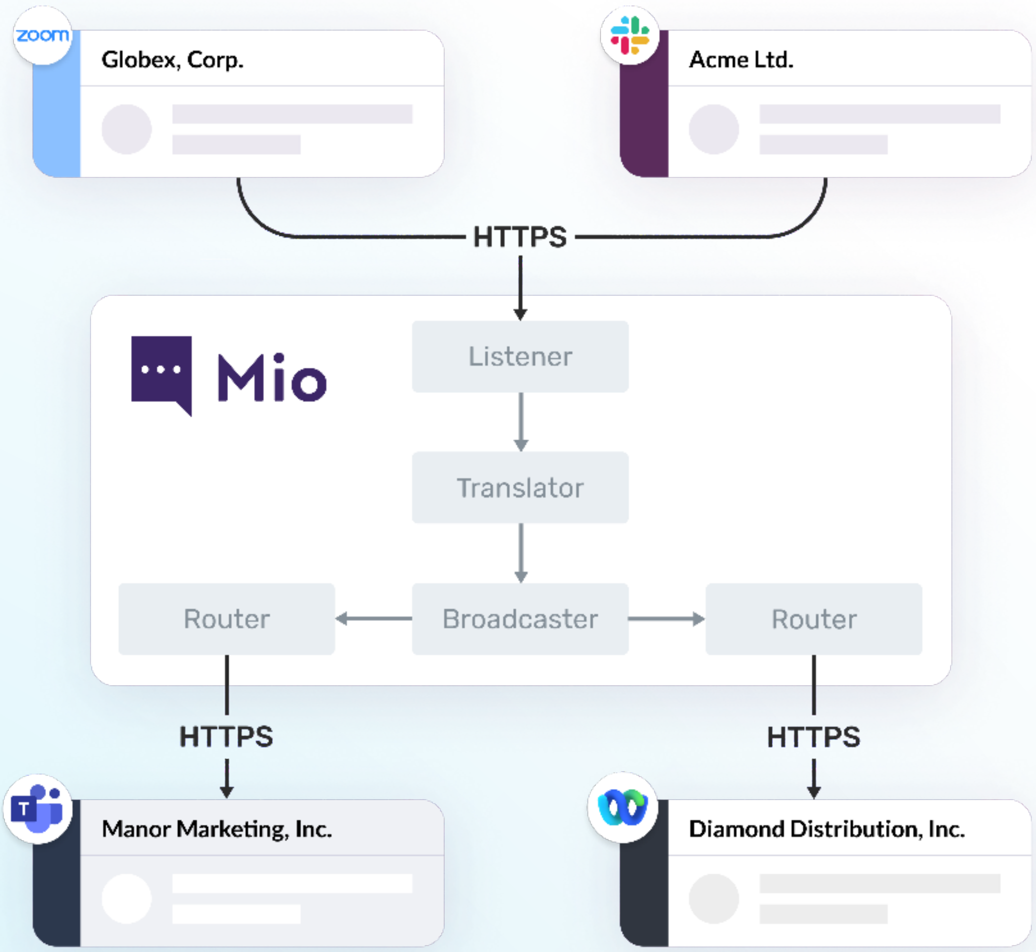
Authorizing access

using AES-256 or equivalent ciphers. We connect to external messaging partners using the strongest grade encryption protocols they support and will proactively upgrade when new standards become available. Data at rest is encrypted to a minimum AES-256 standard at the vendor layer with additional controls applied at the application level for sensitive data.

Network security

Public access to Mio is restricted to a limited number of front-end servers with the minimal number of open ports required to operate our service. The Mio service is run on tightly controlled private networks which are proactively monitored and reported on. Internal access by Mio's employees is tiered, logged and restricted by IP and VPN, and we always work on a principle of least privilege.

Mio has partnered with ThreatStack, an industry leader in cloud security and compliance. Our deep integration means our production systems are proactively monitored and reported on 24 hours a day and any potential issues or concerns are dealt with and escalated by trained SOC engineers immediately.



Software security

Our servers and systems are actively monitored and are regularly updated with the latest security updates as needed. Any errors or omissions found in our own applications are proactively patched and retested at the earliest opportunity. All new servers are hardened before deployment to minimize accidental exposure to potentially insecure default services or credentials. Mio periodically invites external auditors to test and report on our system in its entirety and any feedback is prioritized and acted upon accordingly.

Change control

All application software built and deployed by Mio is subject to version control as part of our secure software development lifecycle. Prior to each production release software is extensively tested and versioned before being made available to the public.

System monitoring and logging

To continuously improve its level of service, Mio may log and inspect traffic passing over its systems. Administrative access by senior members of the team is required to access this information. Mio proactively monitors infrastructure for potential threats and possible data exfiltration.

Legal compliance

Mio has its own internal guidelines towards data privacy and security to help ensure it meets its legal, ethical and socially responsible obligations. Additionally, Mio commissions dedicated legal professionals when needed to help meet legal and regulatory requirements.

Data requests

By default, Mio will minimize personal data collection and retention. For operational purposes, Mio does require a connected user's name and email address to be retained for the life of the service, or until that user or owning organization requests its explicit removal. If Mio receives requests from users or government agencies to disclose or delete data outside of its regular day to day operations, we will meet all legal obligations deemed necessary by our legal counsel.

FAQs

Does Mio store my files and messages?

Mio does not persistently store user messages or files. Message meta data is retained by Mio for future reconciliation across platforms. However the underlying messages and files are not permanently retained.

What message metadata does Mio store and how long is it stored for?

We store the following metadata: message identifier (ID), time stamp, platform assigned user IDs and/or channel IDs and associated identifiers. These are stored for the duration of the service contract, or until Mio is asked to destroy it via a hard delete.

When my user uploads a file where does it go?

Mio provides a proxy service for all files uploaded. When a file is either uploaded or requested by a connected platform or user, Mio will connect and authenticate to the source platform and request the file. As the file is streamed, an outbound connection is made to the target platform or authenticated user, and the file is proxied to the recipient. Occasionally, a real time stream between the platforms is not possible. In this scenario, the file is requested and temporarily cached on the Mio server before the outbound connection is made. This two part transmission is still achieved through a single transaction, ensuring that the file is not retained by Mio outside the transfer session.

FAQs

Does Mio encrypt all data?

When data is in transit between connected platforms, Mio will connect to the API using TLS 1.2 or later, typically over the HTTPS protocol. For data at rest, data will be encrypted with a minimum industry standard of AES-256 encryption. Mio classifies all customer data, and as a minimum all our persistent storage has file storage encryption enabled. For higher classified data, we will perform additional encryption at the field level using an HSM backed AWS KMS service.

End-to-end encryption between platforms via Mio is not currently possible because Mio must be granted access to a plain text version of the chat message in order to translate it to the target platform. Unless chat platforms themselves choose to adopt a universal messaging format, Mio will require temporary access to the raw underlying message to be able to translate and apply the correct markup for the target.

Messages processed by Mio are never stored in an unencrypted format. Inbound events are immediately encrypted and only decrypted on demand when a transformative action is required. Translation typically occurs in milliseconds and in memory, greatly limiting exposure and potential attack vectors. Once translation and delivery is complete, the original and translated payloads are destroyed.

Where is Mio hosted?

Mio is currently hosted exclusively in AWS data centers in the United States of America. We utilize multi-zone redundancy to maximize availability and uptime. All customer data is currently retained in the US.

If AWS fails in one region, does Mio move over to another?

Mio utilizes multi-zone redundancy to maximize availability and uptime.

Can I choose which region my data is stored in?

No, Mio is currently hosted in the US and we reserved the right to fail over to any AWS data center as part of our established business continuity plan.

What happens to messages when Mio is down or when platform APIs are down?

To maximize Mio's message delivery reliability, we've implemented a number of flow controls for messages entering and leaving the Mio subsystems. All message events received by Mio are delivered to front end servers distributed over multiple availability zones. For resilience, event payloads are immediately encrypted and placed into a fault tolerant FIFO queue for processing by the Mio multi-zone, distributed back end system. Mio has distributed its infrastructure and processing logic in such a way that processing and data persistence is highly resilient to individual node or cluster outages.

Mio's ability to deal with partner outages requires an inbound and outbound replay strategy. Partners such as Slack have an automatic redelivery mechanism where, should a Mio resource be unavailable, they will resend the event multiple times until successful or they will otherwise give up. Mio's outbound reliability is defined by our own queue replay strategy. Should a target partner platform be unavailable, Mio will retain the encrypted event in a queue, and will automatically attempt redelivery based on a time based replay strategy. Permanent failures are reported internally and monitored for further investigation and escalation where necessary.

How does Mio work with regards to data loss prevention?

Mio currently employs ThreatStack to proactively monitor all of its production servers and infrastructure 24 hours a day. Agents are installed on every production instance and look for system anomalies and possible attempts of data exfiltration. A tested and proven escalation process is in place for Mio staff to react to any concerns that might be raised.

FAQs

What are Mio's policies regarding data retention?

Mio retains customer data for the duration of their active account. The customer may request their data to be permanently deleted at any time (subject to Mio adhering to applicable state and federal laws).

What are Mio's policies regarding personally identifiable information (PII)?

Mio retains the following PII information for the purpose of normal operation of the service: First name, last name, email address and avatar (if available). Mio will also be provided an end user's exposed public IP address when accessing the m.io website.

Which app scopes does Mio need?

Mio securely integrates with your messaging platforms and never asks for more permissions than necessary to make the app function as intended. Read more about each scope and why we need them in our Help Center.

Where can I find more information about Mio's security practices?

For more information about Mio's security practices, visit our Help Center.

Have more security questions?

Schedule a call with a member of our security and data privacy team.

Interested in a security review with us?

SOC-2 Type II reports, penetration test reports, and more are available upon request.

Chat better, together.