2020 Security White Paper

Our approach

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 document presents our transparent approach to security so your company can have a high degree of confidence when communicating over our systems.

Security by design

It is our philosophy that security should be incorporated in to 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 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.

Protecting your data

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.

Data encryption in transit and at rest

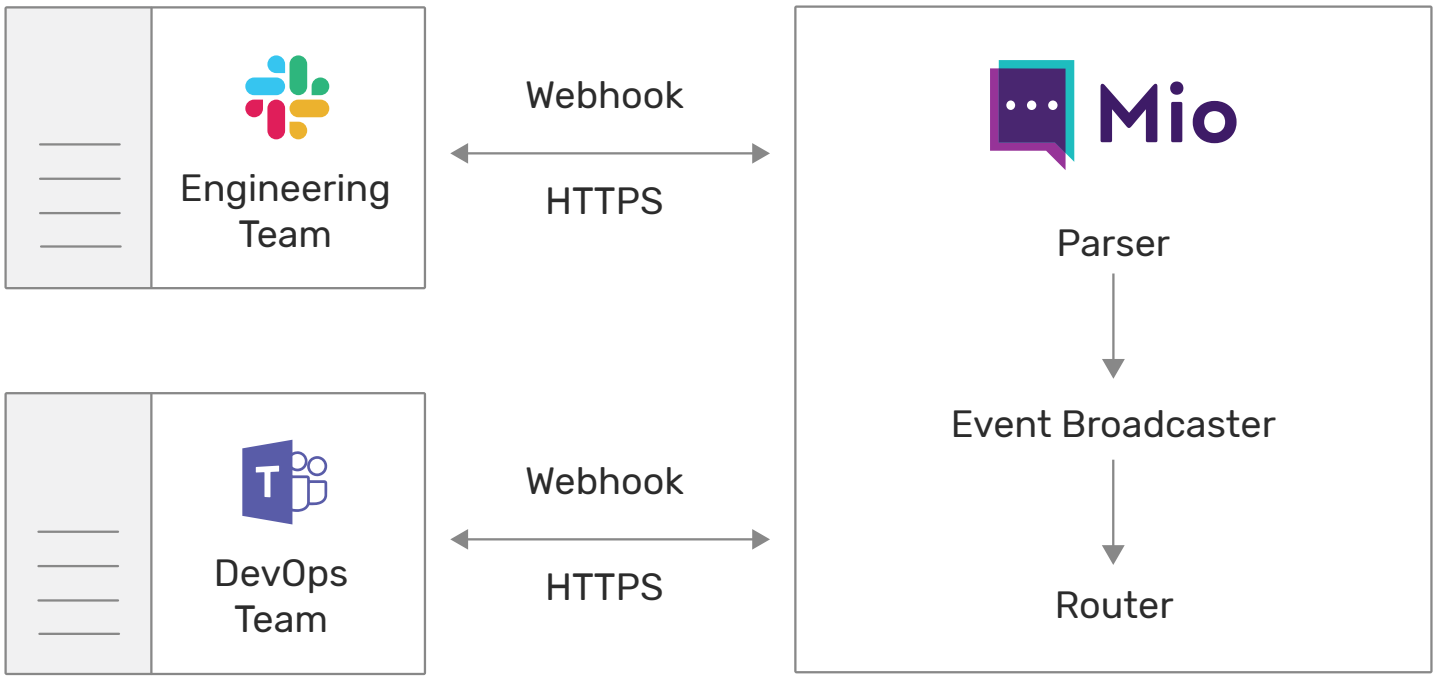
All data that is transmitted via Mio systems uses the TLS 1.2 protocol and sensitive payloads are encrypted using AES-256 or equivalent ciphers. We connect to external messaging partners using the highest supported encryption protocols they support and will proactively upgrade when new standards become 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

We do not store plain text passwords or similar sensitive credentials on our system. Whenever possible we require users to use our platform partners authentication systems and as a result only process and store encrypted tokenized access credentials for each of our users.

Network security

For customers relying on our dedicated managed hosting, Mio isolates each tenant within its own personal private network and provide a set of dedicated and isolated services for maximum privacy, security and compliance. 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. Internal access by Mio's employees is tiered and restricted by IP and VPN credentials and we work on a principle of least privilege.



Safe and secure

Mio securely integrates with your messaging platforms and never stores messages or files.

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 tries to minimize personal data retention and typically only stores highly anonymized or obfuscated data on its systems. 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.