message monkey

Security Whitepaper

APRIL 2024

Overview

MessageMonkey is a service providing low-latency cross-platform interoperability for Slack and Microsoft Teams. Our unwavering commitment lies in safeguarding the **privacy**, **confidentiality**, **integrity**, and **availability** of your data.

Every facet of our product has been carefully designed to adhere to the Principle of Least Privilege and align with international guidelines on data privacy and protection. We constantly work on maintaining and improving our security posture.

Privacy

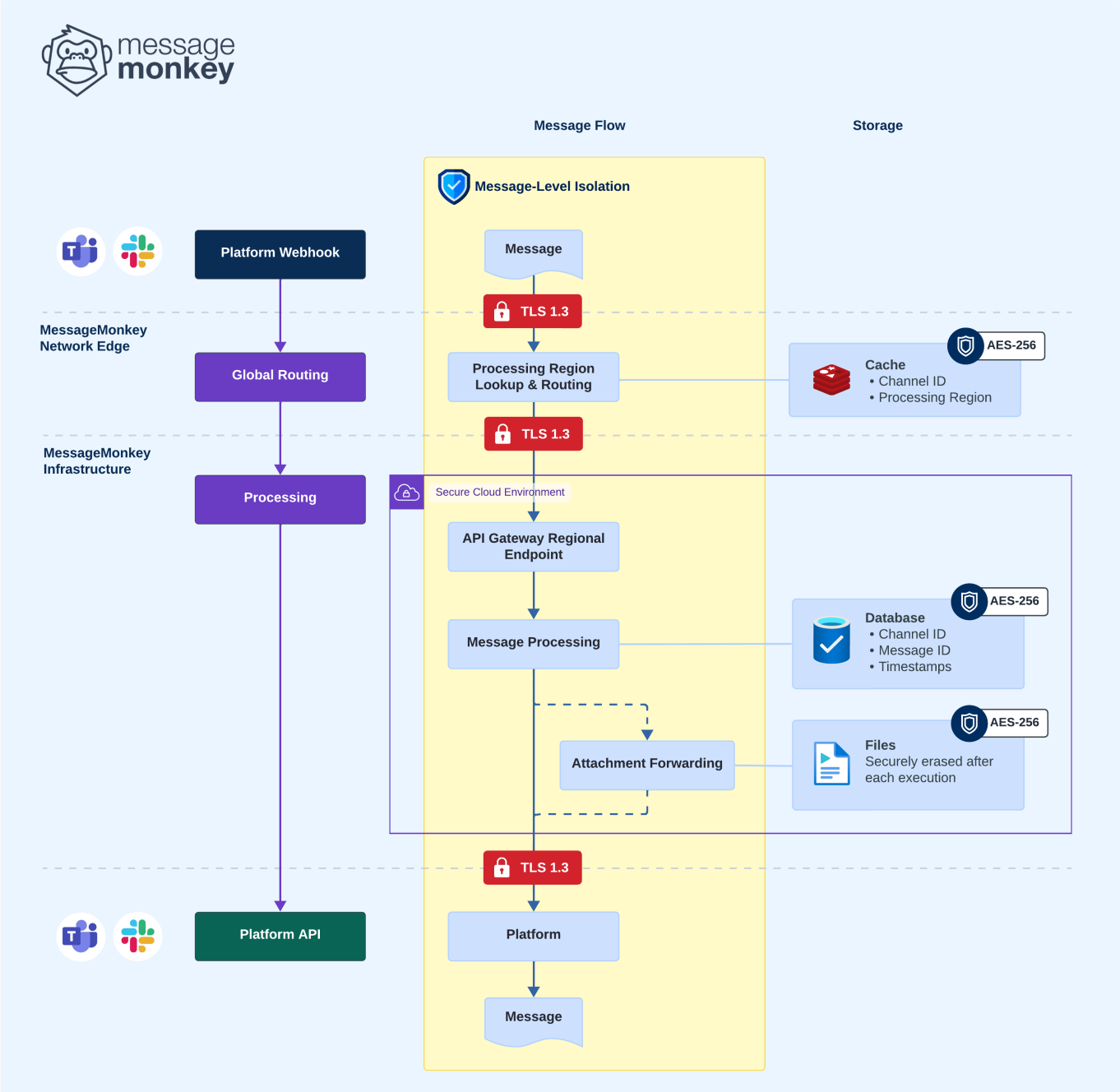
We comply with international data protection regulations, including the EU & UK General Data Protection Regulation (**GDPR**), Singapore's Personal Data Protection Act (**PDPA**), and the California Consumer Privacy Act (**CCPA**).
Our privacy policy is transparent and accessible, outlining our data collection and usage practices.

MessageMonkey adheres to GDPR's requirements, the toughest privacy and security law in the world.

We also safeguard all personal data according to Singapore's PDPA compliance standards.

We have implemented organisational controls to uphold the digital privacy rights of your users under the CCPA.

Designed for Security



Each message we handle is processed in isolation, ensuring that your data is never inadvertently shared with another customer. We encrypt data both at rest and in transit and we only retain the bare minimum data required to deliver our services. We wipe all residual data between invocations of the message flow.

Confidentiality

DATA ENCRYPTION

All data transmitted between MessageMonkey and connected platforms is encrypted using industry-standard TLS 1.3 encryption. This ensures that your messages and files are protected from unauthorized access during transit.

Additionally, all data stored by MessageMonkey is encrypted at rest using AES-256 or equivalent encryption ciphers.

ACCESS CONTROL

We do not store any passwords or sensitive credentials on our system. When you connect your Slack or Teams account to MessageMonkey, we use OAuth 2.0 to authenticate your account and obtain tokenized access to the APIs.

Tokens are securely stored and encrypted in our database.

NETWORK SECURITY

MessageMonkey's infrastructure is protected by multiple layers of security, including firewalls, intrusion detection systems, threat detection systems, and DDoS protection. Internal access by MessageMonkey employees is strictly controlled, monitored and logged.

MessageMonkey leverages AWS and Cloudflare's industry-leading security features to protect against threats and vulnerabilities.

ORGANIZATIONAL SECURITY

Access to our production environments is strictly limited to a select group of senior engineers. Our architecture is designed such that deployments are automated and production access is not required for routine operations.

We also uphold a strong commitment to security awareness among all employees. Regular security training sessions are conducted, and we enforce rigorous security policies to ensure the secure and responsible handling of your data.

Integrity

CHANGE CONTROL AND SOFTWARE DEVELOPMENT LIFECYCLE

MessageMonkey uses a robust software development lifecycle that includes code reviews, automated testing, security testing, and continuous integration and deployment.

All changes to the codebase are tracked, reviewed, and tested before deployment to ensure that they do not introduce vulnerabilities or compromise the integrity of the system.

DATA AUTHENTICITY

All communications from various platforms to MessageMonkey are safeguarded using TLS 1.3 encryption and validated with HMAC signatures.

This dual-layered security measure guarantees that messages and files remain untouched during transmission, thereby preserving the authenticity and integrity of the data.

Availability

HIGH AVAILABILITY ARCHITECTURE

MessageMonkey's workloads run on a highly available, serverless architecture. This robust design allows our service to automatically scale and handle high volumes of traffic, ensuring consistent availability even during unexpected surges in demand.

This architecture is also resilient to physical failures, as it is distributed across multiple AWS datacenters in each region.

MONITORING

We employ a comprehensive monitoring system that persistently assesses the health and performance of our services. This system promptly notifies our Site Reliability Engineering (SRE) team of any irregularities or potential problems.

Our proactive approach enables us to rectify issues promptly, ensuring uninterrupted availability of our service.

Frequently Asked Questions

Can I choose which region my data is processed in?

Yes. MessageMonkey operates from three AWS regions: Virginia, Frankfurt, and Singapore. When setting up a new channel pairing, you'll be able choose your preferred region. After the channel pairing is activated, messages are intelligently routed through Cloudflare's global network edge to your selected region, ensuring that your data is processed in the location of your choice.

If platform APIs are unavailable, what happens to the messages?

In the case where MessageMonkey is unable to reach a platform's (i.e. Slack or Teams) API, our message delivery system uses an exponential-backoff retry mechanism at each step of the process. When the platform APIs come back online, the request then succeeds and the process will resume until the message is successfully delivered.

What happens if MessageMonkey is down?

MessageMonkey's infrastructure is built to handle thousands of concurrent requests. Every component from the network edge to the API Gateway to the message processing layer is designed to be highly available; distributed across multiple datacenters and able to automatically fail over without interruption.

Should MessageMonkey's resources be unavailable, platforms such as Slack and Teams will automatically redeliver messages multiple times until successful or the limit of retries is reached. MessageMonkey's Site Reliability Engineering team monitors the platform for failures around the clock and takes proactive steps to minimise any downtime.

Frequently Asked Questions

What data does MessageMonkey store?

At MessageMonkey, we prioritise your data privacy. We do not store the content of any messages. Instead, we only retain metadata, which includes elements like message IDs, timestamps, and platform IDs. This practice allows us to track message delivery effectively without compromising on data security. This policy is uniformly applied across all our data storage systems, including databases and logs.

In order to facilitate features such as mentions and direct messages, as well as handle billing processes, we securely store certain user information. This includes user IDs, names, avatars and emails of those who are listed in connected channels, if they are available. We ensure this data is always encrypted, both during transmission and when stored, providing an additional layer of security.

What are your data retention policies?

MessageMonkey retains customer data for the duration that the customer account is active. When a customer deletes their account, all data associated with that account is deleted from our systems.

How does MessageMonkey handle file uploads?

When a file is uploaded or requested by a connected platform or user, MessageMonkey initiates a secure connection to the source platform, authenticates, and requests the file. The file is temporarily held in a secure, encrypted cache before the outbound connection is established.

Once the file has been successfully transferred, it is immediately deleted from the cache. This two-step process is completed within a single transaction, ensuring that MessageMonkey does not retain the file beyond the duration of the transfer session.

Frequently Asked Questions

How does MessageMonkey ensure data privacy?

MessageMonkey is committed to protecting the privacy of your data. We adhere to the Principle of Least Privilege, which means that only the minimum amount of data necessary to provide our service is collected and stored. We also encrypt data in transit and at rest, and regularly review our security practices to ensure that your data is safe.

Does MessageMonkey comply with GDPR and other data protection regulations?

Yes, MessageMonkey is fully compliant with EU GDPR, UK GDPR, Singapore's Personal Data Protection Act (PDPA), and the California Consumer Privacy Act (CCPA).

Does MessageMonkey have a disaster recovery plan?

Yes, MessageMonkey has a robust disaster recovery plan in place. Our architecture is designed for high availability and is distributed across three physically separate datacenters in each of our AWS regions. These datacenters are strategically located to ensure that they are not affected by the same natural disasters or power outages. This design ensures that our services remain accessible even if one datacenter encounters issues.

In the rare event of a regional outage, our disaster recovery plan involves failing over to a nearby region. This failover process is temporary and lasts only until the primary region has fully recovered. This strategy allows us to maintain service continuity and minimise disruption to our users.

What is MessageMonkey's policy on third-party data sharing?

MessageMonkey is committed to protecting your privacy and data. We will never share your data with third parties.

NOTICE

Informational Purpose: This document serves informational purposes only.

Subject to Change: It reflects current MessageMonkey product offerings and practices, which may change without notice.

No Commitments or Assurances: This document does not create any commitments or assurances from MessageMonkey or its affiliates, suppliers, or licensors.

"As Is" Basis: MessageMonkey products or services are provided "as is," without warranties, representations, or conditions, whether express or implied.

Legal Governance: The responsibilities and liabilities between MessageMonkey and its customers are governed by MessageMonkey agreements. This document does not modify any existing agreement.