POLYMER

2021 Security White Paper

OUR APPROACH

Polymer secures 3rd Party SaaS platforms. In doing so, protecting the integrity and security of your data is of the highest importance to us. This document presents our transparent approach to security so your company has a high degree of confidence when using our platform.

Zero-Trust, from the Grounds up

Polymer is purpose built with the highest security protocols in the market. The infrastructure and operations of the entire organization was tested under Covid in a remote work environment. All projects are designed with a security assessment as the initial and final step before go-live. Polymer is SOC2 Type I compliant and is under review for Type II approval middle of 2021.

Human-centric security

Every team member needs to pass security courses from coursera on a quarterly basis. We expect all engineers to be security proficient and fluent in the latest threats as part of their job. All laptops and end points are accessible via VPNs and rotating tokens. No engineer has access to customer data-ever.

Protecting Customer 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 Polymer systems uses the TLS 1.2 or later, and sensitive payloads are encrypted using AES-256 or equivalent ciphers.

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

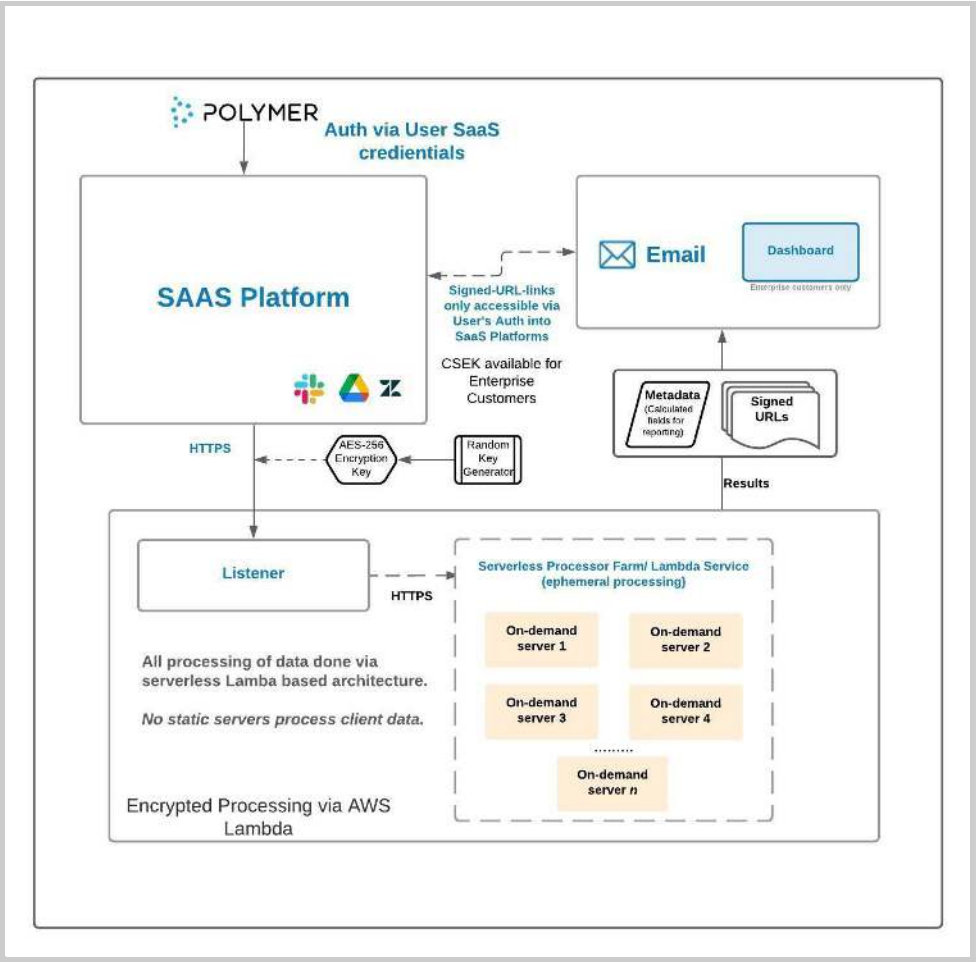
We do not store plain text passwords or similar sensitive credentials on our system. We require end users to use our platform partners SSO authentication systems and as a result only process and store encrypted tokenized access credentials for each of our users.

Network security

Public access to Polymer is restricted to a limited number of front-end servers with the minimal number of open ports required to operate our service. The Polymer service is run on tightly controlled private networks which are proactively monitored and reported on. These networks cannot be accessed from outside IP addresses. Internal access by Polymer's employees is tiered, logged and restricted by IP and VPN, and we always work on a principle of least privilege.

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. Polymer periodically invites external auditors to test and report on our system in its entirety and any feedback is acted upon accordingly.

Change control

All application software built and deployed by Polymer 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.

To continuously improve its level of service, Polymer may log and inspect traffic passing over its systems. Polymer securely integrates with your messaging platforms and never stores messages or files. All files that are needed for redaction/permissioning within platforms are stored in encrypted format using AWS KMS key that is rotated weekly. Polymer proactively monitors infrastructure for potential threats and possible data exfiltration.

Customer Data Storage & Retention

For our enterprise customers, we also have a CSEK offering to use customer KMS.

The only customer data stored is the metadata around user emails, groups, channels, access levels

System monitoring and logging

for a given organization. Only email is stored unencrypted but the rest of the 'header' data is hashed at the database level. CTO is only administrative access to this database.

For our enterprise customers, this hash function can be tied to the CSEK (customer key).
is required to access this information.

Legal compliance

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

Data requests

By default, Polymer tries to minimize personal data retention and typically only stores highly anonymized or obfuscated data on its systems. If Polymer 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.