How Optimizely encrypts customer data at rest

Skip Ahead

Definitions
- Data stores encrypted at rest
- Data stores not encrypted at rest

relevant products:
- Optimizely Web Experimentation
- Optimizely Web Personalization
- Optimizely Web Recommendations
- Optimizely Full Stack

THIS ARTICLE WILL HELP YOU:
- Understand how Optimizely helps protect your data in the event of a data breach

In order to help reduce customer exposure to data breaches, Optimizely encrypts most product data at rest. This provides an extra layer of protection for much of your Optimizely-stored data.

However, some data sent to our backend systems, such as our CRM and analytics platforms, is not encrypted at rest. For example, neither analytics data collected about collaborators’ use of the product, nor analytics data collected about the performance of the Web Experimentation Javascript client, are encrypted.

This article describes Optimizely's encryption at rest practices for our subprocessors. If you need more information, contact your Customer Success Manager.
Definitions

- **Product data** is data submitted to Optimizely, such as experiment definitions and collaborator contact information.
- **Collaborator analytics data** refers to analytics data collected about collaborators’ use of the product.
- **Performance analytics data** is limited performance data, such as latency, collected about the Web Experimentation client.
- **Visitor data** refers to data concerning the characteristics and activities of site visitors collected by Optimizely.

Data stores encrypted at rest

<table>
<thead>
<tr>
<th>Subprocessor</th>
<th>Product Data</th>
<th>Visitor Data</th>
<th>Collaborator Analytics Data</th>
<th>Performance Analytics Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Web Services, Inc.</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Google, Inc.</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zendesk, Inc.</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auth0, Inc.</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chart.io</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Castle Intelligence, Inc.</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Heroku, Inc. (a Salesforce company)

Pendo, Inc.

Segment.io, Inc.

Looker

Slack

Sentry.io

Marketo

Data stores not encrypted at rest

<table>
<thead>
<tr>
<th>Subprocessor</th>
<th>Type of data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Product Data</td>
</tr>
<tr>
<td>Salesforce</td>
<td>✓</td>
</tr>
<tr>
<td>SendGrid, Inc.</td>
<td>✓</td>
</tr>
</tbody>
</table>

Customer data is processed by Sendgrid only to send emails to
collaborators and track email analytics. It is not stored for more than 30 days.

New Relic ✔

Amplitude ✔