4Thought Marketing Cloud Apps Security Document

Summary & Overview

4Thought Marketing's Cloud Apps typically store no data or only store data briefly, utilize redundant AWS servers with automatic failover, only communicate via 256-bit encrypted protocols, all authorized via the Oracle Eloqua security system, which uses the OAuth 2.0 authorization framework. We also comply with many privacy laws, including GDPR and CCPA, and have well-established and managed internal security policies.

This industry standard approaches, along with the details below, make 4Thought Marketing Cloud Apps highly secure and reliable.

Authentication

Summary:
Cloud Apps built for Eloqua rely on Oracle Eloqua's security system for access and control. In all but 3 apps, 4Thought Marketing cannot see, store, or access Oracle Eloqua passwords. The apps use Oracle & OAuth 2.0 token technology to receive authorization from Oracle Eloqua.

The two apps we have that do store data are:

1. **4Comply** - the module to address the "Right to Portability" stores temporary files during the short processing period of transfer from Eloqua before receipt by an end-user. Access to such files is only available via an encrypted link via a URL shortener/encrypter methodology and after identity verification.
2. **CO Deleter with Archive** and **Contact Deleter with Archive** – sometimes, customers configure these apps to store backup/archive data files temporarily on our servers. However, customers can configure the program to store this information on a customer-supplied Secure (SFTP) Server. The customer chooses where to store this archive.

Specifics:
4Thought Marketing apps do not store Eloqua login credentials because all Eloqua cloud apps authenticate using OAuth 2.0, following the Oracle Eloqua Cloud App Framework. The OAuth 2.0 identity confirmation framework is one of the top two most commonly used authorization frameworks globally.

This framework provides a three-legged authentication process where Eloqua provides authorization codes, access tokens, and refresh tokens that enforce a validation with the Eloqua server and the specific endpoints listed in the App definition within Eloqua.

Even if a "bad actor" were to obtain these tokens, no breach could occur because:

a. Eloqua would only send out a new auth code to the endpoint defined in the app definition
b. That endpoint could only be 4Thought Marketing.

Eloqua Cloud Apps developed by 4Thought Marketing require a user name and password for their initial configuration. Before a user can self-register into the cloud app portal, they must:

1. Have approval from an Eloqua system administrator
2. Eloqua instance has user configured
3. They must authenticate using the OAuth 2.0 process defined above.
4. Portal uses SHA256 (HMACSHA256) hashed passwords for access control.

Note that Oracle Eloqua is fully SaaS 70 certified and has many other documented security protections regarding password lengths, requirements to change them, utilize 2nd-factor authentication if desired. For full details on Eloqua's security, it is best to contact Oracle directly.

Cloud App Data Storage

4Thought Marketing's Cloud Apps rely on Eloqua's Custom Objects for storage of any PII. Again, Oracle Eloqua's environment is highly secure and attendant to several security standards. An option exists for Eloqua users to have data at rest encrypted if desired.

The cloud apps database only stores app configuration and summarized logs of app executions. Neither PII data nor logins are stored in this database. The configuration data is stored in an Amazon RDS SQL Server environment and is only accessible from our application servers' same Virtual Private cloud. AWS is considered one of the most secure environments globally, and more information is available from Amazon regarding SaaS certification, physical environments.

Data Transfer

Oracle requires that all data passed between it and its cloud app vendors like 4Thought Marketing be fully AES 256-bit HTTPS encrypted the same as any other Eloqua data transfer and the same as banks require. For Cloud actions, cloud content, cloud decision, and other apps, Eloqua only sends out notification requests and authorization tokens to the endpoints configured in the app definition.

Cloud App Infrastructure

AWS Environment

4Thought Marketing Apps are hosted in servers with AWS, as part of a virtual private cloud (VPC), each server has its security group within the VPC through which we control access to specific ports and can provide IP Allowlisting.

Redundancy and Automatic Failover

4Thought Marketing Server architecture includes redundancy and automatic failover capabilities to ensure optimal operational performance even at high load times.

SSL Certificates in port 443 secure public interfaces and endpoints. Access is also restricted to RDP or Telnet, FTP, or SFTP Allowlist IP addresses.

No data is stored in the application servers. Application configuration and logs are stored in databases under Amazon Relational Database Services (RDS), and access to the database is only allowed from within the VPC.

Access to the AWS environment is enforced by Two-Step authentication.

GDPR Considerations
4Thought Marketing typically agrees to EU/GDPR "Model Clauses" that allow EU information to be moved out of the EU when requested/necessary for our customer's benefit.

Exceptions:
There are two exceptions to the above policies.

1. This first exception can only be permitted by a customer:

The Contact and CDO Deleter with Archive app can be configured to store backup/archive data files temporarily in our servers. However, it can also be configured to only store this information on a Secure (SFTP) Server provided by their IT department. Where this archive is stored is their configuration choice.

2. The second only occurs during temporary processing, for the very limited specific EU Citizens that are exercising and in the process of downloading their "Right to Portability" data.

Our GDPR Right to Portability app stores temporary files during the short processing period of transfer from Eloqua prior to receipt by an end user. Access to such files is only available via an encrypted link via a URL shortener/encrypter methodology.

4Thought Marketing Cloud Apps Security Processes

Processes Overview
These processes describe how 4Thought marketing Cloud Apps are:

1. Registered by 4Thought with Oracle
2. Configured by a User
3. Used Daily

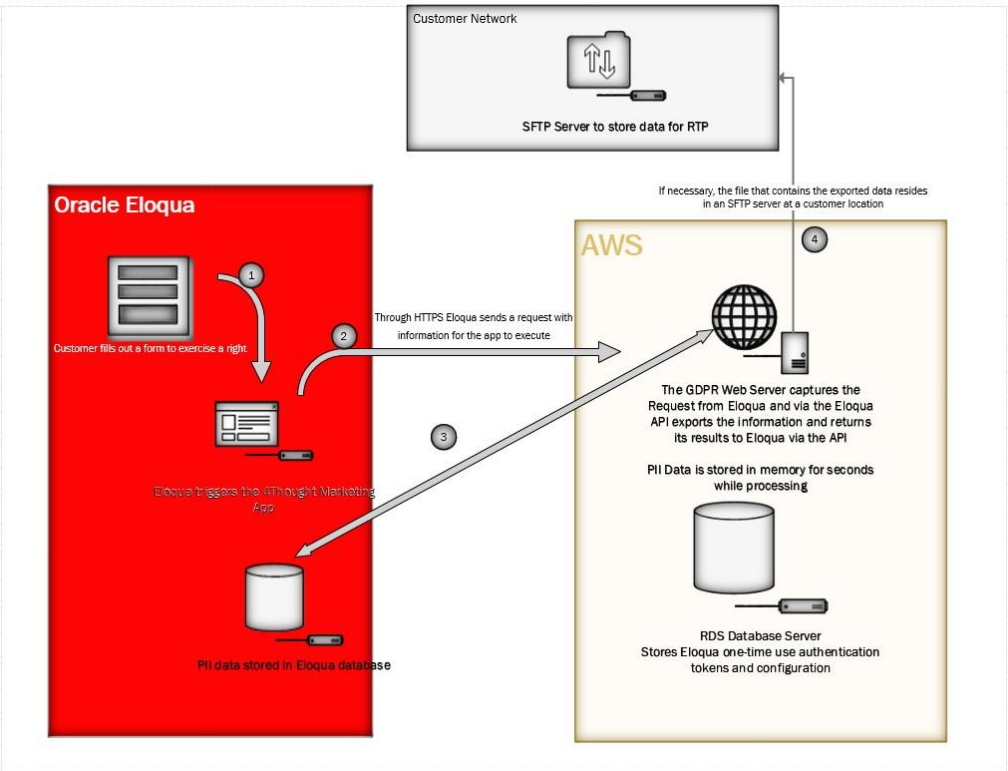
1. Registered by 4Thought with Oracle
   a. 4TM Cloud App is registered with Oracle.
   b. Authorized App Endpoint is stored in Oracle's systems. This endpoint consists of authorized HTTPS URLs, all of which require an SSL certificate. This authorization process of the cloud app can't be used except at these endpoints stopping any man-in-middle attacks.
   c. Thorough testing of endpoints and functionality is performed by Oracle for all Certified Apps
2. User Configures App
   a. User Logs into their specific Eloqua customer licensed version. Full Oracle login security is required to start this process.
   b. Authorized user/customer installs the 4TM Cloud App directly from Oracle-Eloqua's Servers
      i. During App installation user is required to reenter their credentials.

ii. OAuth token is generated and sent to 4TM via encrypted HTTPS for this customer/instantiation OAuth token is stored by 4TM but is only usable for the specific endpoint specified during original app registration d. OAuth token is used to authenticate all future communications between 4Thought Marketing and Eloqua in Daily App Usage 3. User drags onto specific Program Canvas or Campaign Canvas

iii. The App User is required to enter 4TM login credentials which are verified at 4TM via HTTPS for App configuration

3. Daily App Usage

a. All requests are via HTTPS and go only to specified endpoints, authorized via OAuth 2.0 Token. b. See existing example diagram:



General Security

4Thought Marketing is dedicated to upholding the highest security and privacy standards for our products qne on behalf of our customers. Non product related security processes include background checks, clean desk policy, mobile device policy, annual confidentiality agreements, disaster recovery plans, password policies, and much more. Information on all of these general security items can be found at www.4ThoughtMarketing.com/Trust.

Reference links

https://aws.amazon.com/compliance/data-privacy-faq/
Oracle Eloqua Cloud App Authentication
Oracle Eloqua Security Features