MAROPOST

180 University Ave
Suite 5002, Toronto, ON
M5H 0A2, Canada

T 888.438.3152
F 647.438.5600
maropost.com

INFORMATION TECHNOLOGY SECURITY BRIEF

V 2.0

Author: Dennis Dayman

Date: Aug 4, 2021

Table of Contents

Revision History

Version	Date	Author	Notes
2.0	Aug-4-2021	Dennis Dayman, Navdeep Singh, Manny Ju	Update document to reflect new cloud hosting provider
1.0	Jan-15-2016	Jagdeep Singh	Initial Release

Overview

Maropost Marketing Cloud is an enterprise-level SaaS based web-application that combines digital messaging campaign list management, marketing automation, and deployment.

The application is offered as a "hosted rich internet application". Users require a modern browser, for example Chrome, Firefox, Safari, or Edge to access it. The browser sessions use a 128-bit encrypted SSL connection. The servers are hosted in a secure, 3rd-party cloud hosting provider's data center with 24/7 monitoring, redundant power supply, and real-time backups complying with international standards for data security and management.

Application Security

Maropost has powerful security controls, including those that allow clients to do the following:

- Specify the IP addresses that users are allowed to send campaigns from
- IP address validation at login
- User-level IP address restriction
- Organizational-level IP address restriction
- Enforcement of industry-standard "strong" password rules including:
    - Must be at least 10 characters
    - Must include at least one capital and one lower-case letter
    - Must include at least one integer
    - Must include at least one special character
    - No 2 characters may repeat in succession
- Optional 2-factor authentication for user login
- Control user actions post-login with multiple permission levels, including:
    - User interface access rights
    - API access rights
    - Individual access rights (add/update/delete contacts, export lists, etc.)
    - Functional access rights (send mailings, view reports, administrative, etc.)
    - File/Folder access rights
    - Database access rights

Application Security is also addressed by keeping client data separate from the application, providing an audit trail of user actions performed on the system and encrypting passwords.

Additional Security Measures

Maropost has implemented security measures outside of the application specifically designed to prevent unauthorized access to the application and to client data. These additional security controls are implemented under the categories listed in this section.

Secure Architecture

The Maropost enterprise network uses servers and networking equipment including firewalls that are maintained by Google Cloud Platform (GCP). Networking equipment is configured consistent with the manufacturers' best practices for operational stability and security, which comes with the latest

firmware. In addition, none of the application and database servers are accessed via any external IP address. All servers operate within the secure, internal network.

Secure Transmissions and Sessions

Connection to the Maropost environment is via SSL/TLS 1.2 ensuring that our users have a secure connection from their browsers to our service. Individual user sessions are identified and re-verified with each transaction, using a unique token created at login required for all communications with Maropost data centers. We offer SFTP with 128-bit encryption standard for all file transfers over FTP, as well as FTPS support for clients who request this option.

Network Protection

Perimeter firewalls managed by GCP block unused protocols. Intrusion prevention and detection sensors report events to a security event management system for logging, alerts, and reports. Internal access control lists segregate traffic between the application and database tiers.

Internal and Third Party Testing Assessments

Maropost tests all code for security vulnerabilities before release, and regularly scans our network and systems for vulnerabilities. Third-party assessments are also conducted regularly.

Monitoring

Our Information Security department monitors notifications from various sources and alerts from internal systems to identify and manage threats.

Data Centers

Our service is hosted by GCP in three of their data centers located in the United States, Canada, and Germany. Customer data for any account is solely located within a single data center. Clients have the option to specify which data center to store their customer data.

Backups

Maropost implements GCP's multi-zone architecture. Databases are installed at multiple physical locations within the same data center (a.k.a. "zones"). Data is replicated between zones automatically in near real-time.

Use of multi-zones obviates the need for off-site data storage. Snapshots are taken on a daily basis and stored within multiple zones with a 7-day retention period.

Disaster Recovery

Maropost's Customer database is replicated in multiple zones within a GCP data center, using master/slave replication strategy.

The databases are asynchronously replicated to slave servers in near real-time. The master databases are in one zone and the slaves in another. This separation ensures failover continuity should one of the zones become unavailable.

Regulatory Compliance

Maropost uses data centers which are and have obtained a GDPR compliant certification of such and also have annual ISO/IEC 27001 audits. The Maropost platform also has its own GDPR complaint certificate which can be obtained upon request.

Incident Response

Incident response is negotiated with each client and is part of its SLA (Service Level Agreement). A standardized version and Inbox SLA is part of the Maropost's policy documentation.

Spam Compliance

Maropost Marketing Cloud is fully compliant with privacy regulations including CAN-SPAM, CASL, GDPR, CCPA, and others. Our Terms of Use establishes zero tolerance for non-compliant usage of our platform. Maropost's Customer Success and Deliverability teams also assist clients with best-practices education to help them remain within compliance themselves.

Policies and Change Management

Change Management is in place to control changes to all critical company and client information resources (such as client data and information, hardware, software, system documentation and operating procedures). The process covers management responsibilities and procedures in addition to employee-agreed to policies, and are subject to audit.

Maropost's comprehensive change control process includes the following phases:

- Logged Change Requests
- Identification, prioritization and initiation of change
- Proper authorization of change
- Data/database access login/out access with full user action audit trail
- Requirements analysis
- Inter-dependency and compliance analysis
- Impact Assessment
- Change approach
- Change testing
- User acceptance testing and approval
- Implementation and release planning
- Documentation
- Change monitoring
- Defined responsibilities and authorities of all users and IT personnel
- Emergency change classification parameters

In addition to the above, Maropost employees are required to sign Non-Disclosure Agreements and Acceptable User Policies. These policies are strictly enforced and frequently audited by our internal operations team. All policies are reviewed with the executive stakeholder responsible for overseeing the work in addition to responsibilities requiring the approval of Maropost's Privacy Officer.

All changes to policy and the subsequent communications to employees and clients are handled by the appropriate executive stakeholder and/or the Privacy Officer.

Business Continuity & Disaster Recovery

Maropost's Business Continuity plan defines the following key points:

- Membership of the Business Continuity Action Team
- Events that trigger the implementation of the Business Continuity plan
- A listing of the Critical Services organizations
- A listing of Critical Suppliers
- Procedures when the Business Continuity Plan is in effect including definition of primary and secondary backup roles.

Maropost implements GCP's multi-zone architecture. Databases are installed at multiple physical locations within the same data center (a.k.a. "zones"). Data is replicated between zones automatically in near real-time. Procedures are in place that define the steps to recover critical systems in the event that one of the zones of a region experiences a failure.