WHITE PAPER

Adobe Marketo Engage Security Overview

August 2024

Table of Contents

Adobe Security

At Adobe, we know the security of your digital experience is important. Security practices are deeply ingrained into our internal software development, operations processes, and tools. These practices are strictly followed by our cross-functional teams to help prevent, detect, and respond to incidents in an expedient manner. We collaborate with partners, leading researchers, security research institutions, and other industry organizations to keep up to date with the latest threats and vulnerabilities. We regularly incorporate advanced security techniques into the products and services we offer.

This white paper describes the defense-in-depth approach and security procedures implemented by Adobe to secure Marketo Engage and its associated data.

About Marketo Engage

Marketo Engage brings together marketing and sales in a single solution designed to orchestrate personalized experiences, optimize content, and measure business impact across every channel, from consideration to conversion and beyond.

Solution Architecture

The Marketo Engage solution includes the following components:

- **Marketo Lead Management** (MLM) — The core of the Marketo Engage application, MLM is where customers launch marketing programs, create campaigns to nurture leads, design landing page and email assets, and report on performance metrics.
- **Revenue Cycle Analytics** (RCA) — Enables users to report on the performance of their marketing efforts, including opportunity attribution, email performance, and lead generation.
- **Web Activity Tracking** — A JavaScript, called Munchkin.js, that customers place on their websites to collect information on page visits and clicks for use in Marketo Engage lead nurturing.
- **Marketo User Interface** — Customers interact with the Marketo Engage solution using the Marketo UI. Administrators use the same UI to authorize Marketo Engage and integration users (see next bullet for more information).
- **APIs** — Enable third-party developers to integrate their solutions with Marketo Engage using REST or SOAP API calls.
- **LaunchPoint Integrations** — Marketo-built and -maintained integrations with webinar providers and ad platforms.

- **Native CRM Integrations** — Marketo-built and -maintained connectors to the Salesforce.com and Microsoft Dynamics CRM platforms.
- **Marketo Sales Insight** (MSI) — App packages that customers can install in their Salesforce or Microsoft Dynamics environments, which allow CRM users to view Marketo Engage lead data and trigger Marketo Engage emails and marketing campaigns.
- **Add-on Modules** — Customers can extend their Marketo Engage solution with one or more of the following Marketo modules, available at additional cost:
  - Sales Connect – Engage sales leads via multiple channels throughout the sales cycle
  - Target Account Management – Target, score, and engage with key accounts
  - Web Personalization –Target key audiences and serve them personalized content
  - Predictive Content – Engage web visitors and email recipients with the most relevant content, using suggestions powered by machine learning and predictive analytics
  - SEO – Track website performance in search engines and provide guidance in improving rankings
  - Marketo Mobile Engagement – Integrate with smart phone applications to track engagement, target audiences, and push notifications

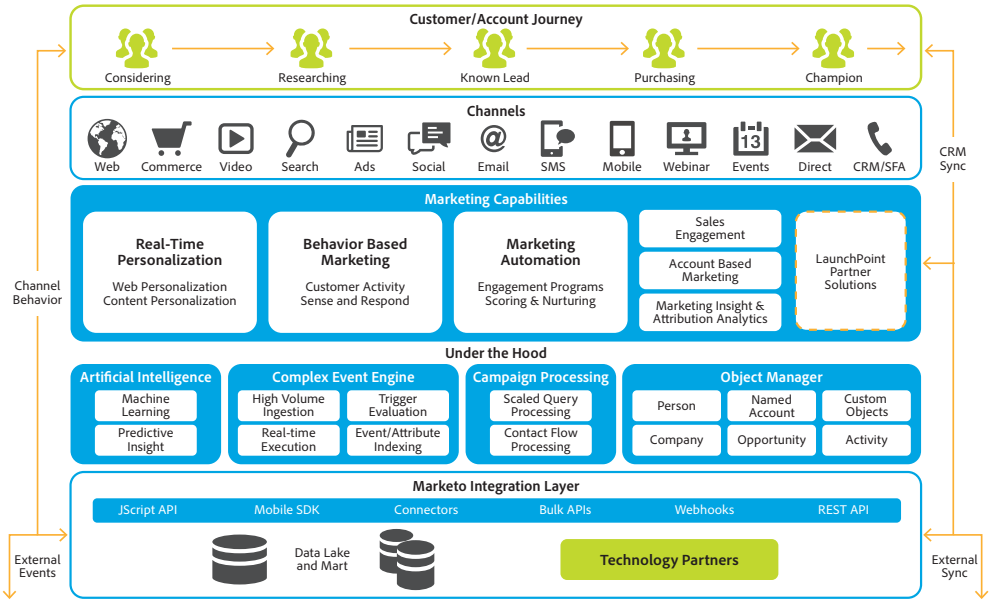


Figure 1: Marketo Engage Solution Architecture

Security Architecture and Data Flow

The following network diagram depicts the Marketo Engage security architecture:

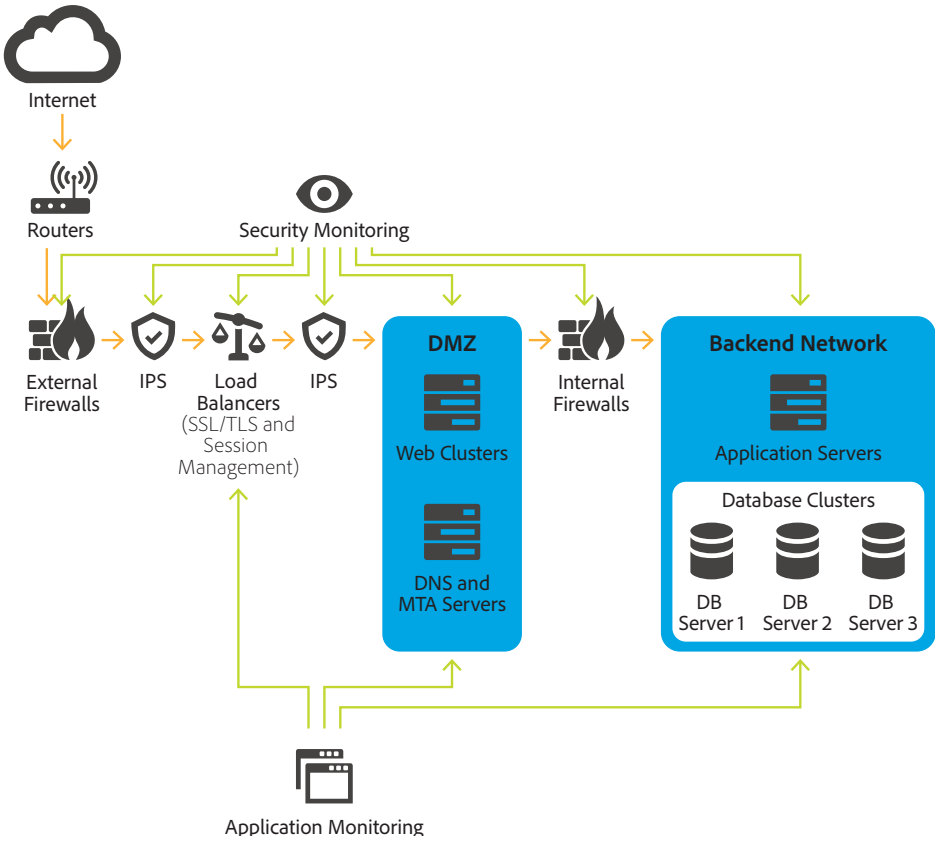


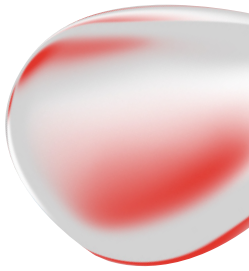
Figure 2: Marketo Engage Network Security Architecture

Data Flow Narrative

The following narrative describes how data flows into and out of a Marketo Engage implementation:

- The customer determines where to deploy landing pages, forms and media, which are supported by the Marketo Engage munchkin.js cookie and other tracking technologies. These forms and tracking technologies collect data from visitors to the customer's website and landing pages, which is then transmitted to and stored in the customer's Marketo database at the applicable data center. Data collected from visitors can include device IP address, geolocation data inferred from IP lookups, and personal data collected by forms.
- Lead data can enter Marketo Engage from external sources managed by the customer. These sources include:
  - List imports – Users can import .csv files of lead data mapped to Marketo Engage lead fields

- REST/SOAP APIs – External integrations may push data into Marketo Engage using publicly available APIs or webhooks
- LaunchPoint integrations – Third-party integrations with webinar providers, ad platforms, social media platforms, and other services approved (but not operated) by Marketo, may synchronize lead and device data between the third-party service and Marketo Engage
- Manual input – Users may manually create and update lead data in the application



- Marketo Engage supports automatic two-way synchronization with Salesforce.com and Microsoft Dynamics CRM platforms. Enabled subscriptions sync lead, contact, account, and other data using internal APIs encrypted via HTTPS.
- Marketo Engage interprets data, such as demographical and behavioral information, stored in the database to nurture leads throughout the marketing and sales lifecycle, including to target audiences for marketing campaigns.
- If a user initiates an email from Marketo Engage to a natural person, lead data can be used to personalize the email content. This data can consist of Personally Identifiable Information (PII) collected by the customer from the person or data maintained by the customer, such as an account number, to facilitate the relationship. In order to enable metrics reporting, such as email open rates as well as IP address, email client, and other device information, data may flow from the recipient of an email back to the customer's Marketo database by means of a tracking pixel embedded in the email.
- Web content, including landing pages, forms, and posts on social media can be dynamically personalized to incorporate lead data in the design, e.g., welcoming a visitor by their first name.
- Marketo Engage users with sufficient permissions can initiate exports of all lead data from the UI for use in external applications.
- If Marketo Sales Insight is installed in an environment integrated with Salesforce.com or Microsoft Dynamics, customer data can flow between the platforms, allowing CRM users to view Marketo Engage-hosted lead data and to trigger marketing campaigns. This data flow utilizes the application's internal APIs and is encrypted via HTTPS.
- Certain processing operations, such as the Predictive Content and Marketo Mobile Engagement offerings, rely upon data service providers, known as sub-processors, for specific and limited feature capabilities. When a sub-processor is used, customer data flows from the Marketo database to the sub-processor and back again after processing.
- If the customer chooses to extend their deployment with one of the Marketo add-on packages, such as Target Account Management or Advanced BI Analytics, lead data flows between them.
- If the customer chooses to deploy a third-party solution that is already integrated with Marketo or uses Marketo's API to integrate with a new third-party or proprietary

[1] The sub-processors applicable to a customer's use of Marketo depend upon which services the customer selects for their package. A list of all sub-processors is publicly available at https://documents.marketo.com/legal/sub-processor-list/.

solution, the data that flows between the solutions depends on the customer's specific implementation.

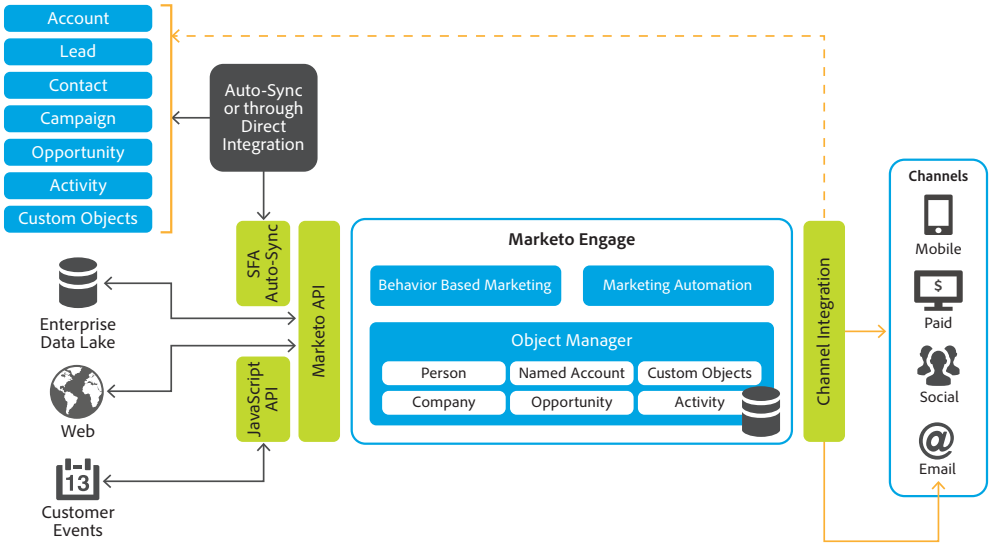


Figure 3: Marketo Engage Data Flow

Data encryption

Marketo Engage uses HTTPS TLS v1.2 to protect data in transit. For an additional fee customers may purchase the ability to encrypt data at rest with AES 256-bit encryption.

User Authentication

Marketo applications are accessible via any browser-enabled client, and support IP range restriction, including allow lists and deny lists. User login and data actions are tracked in audit logs. Session timeouts automatically log an idle user out of the applications. SaaS instance administrators can set password strength parameters that enforce length, case, mixed case, number, special characters, and expiration.

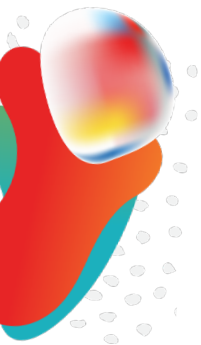
To prevent password-guessing (brute force) attacks, account access is locked automatically after five (5) unsuccessful attempts to guess a password.

Marketo also supports customers' enterprise Single-Sign-On (SSO) using SAML v2.

Additional Security Customizations

Marketo Engage enables the following additional controls:[2]

- **Role-based access** — Marketo users are granted role-based access by the administrators. Access permissions are based on assigned user roles, which specify security rights for normal users, power users, and system administrators. In addition to predefined roles, administrators can create additional roles, with more than 100 available access permissions.
- **Access segmentation** (Workspaces) — To restrict data access based on data values, Marketo administrators can implement workspaces. For example, users can be given access only to accounts or regions assigned to them.
- **Device authorization** —Customer logins to the Marketo solution from unrecognized network locations trigger a device authorization check in the form of an additional token verification, in which a token is sent to the account's registered e-mail address for validation.
- **IP restrictions** — Marketo supports customer-controlled allow listing or deny listing of specified IP addresses and networks.
- **Configurable password parameters** — Administrators can configure complexity, length, limited attempts and expiration of user passwords.
- **Antivirus** — Antivirus checks and blocking of potentially unsafe files are performed on all uploaded data.
- **Account creation notification** — Administrators are notified when a new admin account is created.
- **High security mode by default** — When a new Marketo subscription is activated, security parameters are set to the most stringent security and can be adjusted as needed by the subscription administrator.
- **Session timeout** — Marketo administrators can configure Inactive sessions timeout.



[2] All customizations except antivirus are controlled by the Marketo Engage administrator. Antivirus is enabled on all subscriptions and cannot be disabled.

Hosting Locations and Security

The Marketo Engage service infrastructure resides in enterprise-class data centers or co-locations from top-tier cloud hosting providers in US-West and US-East, Ireland, and Australia, as well as in an Adobe-managed data center in The Netherlands.

All data centers provide the full range of hosting facility features, such as fully redundant power and environmental systems as well as industry-leading and third-party audited levels of security.

Figure 4: Marketo Data Center Locations

Questions?

For more information about Adobe's operational, application, and enterprise security processes, compliance certifications, incident response program, security training and awareness program, and business continuity and disaster recovery program, please see the Adobe Trust Center.

Adobe

08/24