WHITE PAPER

Adobe Marketo Measure Security Overview

July 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 Measure and its associated data.

About Marketo Measure

Marketo Measure (formerly Bizible) is the market-leading revenue attribution and planning software for B2B companies that want to understand how their marketing efforts are driving downstream revenue so they can impact future revenue, justify spend, and make smarter data-driven decisions.

By unifying behavioral and ad data with sales outcomes and machine learning, marketers can get actionable insights and ultimately make accurate, informed marketing decisions. From first touch to close, across all marketing channels, Marketo Measure enables marketers to connect marketing to revenue through advanced analytics.

Solution Architecture

There are three (3) primary components that track, organize, and house data and provide reporting capabilities in Marketo Measure. These components include:

- **Marketo Measure JavaScript** — The Marketo Measure JavaScript (bizible.js) tracks all the online marketing interactions, also called touchpoints, that prospects/leads have with the customer's organization. It is a custom script that is added before the closing </head> tag on every marketing page of the customer's website, e.g., *<script type="text/javascript" src="//cdn. bizible.com/scripts/bizible.js" async=""></script> bizible.js* captures data from web visits (including anonymous web visits), general traffic/page navigation, content downloads, and form submissions. The Marketo Measure solution processes this data for the customer and pushes it into their customer relationship management (CRM) solution, with each marketing interaction displayed as an online touchpoint.
- **Marketo Measure Application** — Customers use the Marketo Measure application to view and report on attribution data, configure account settings, and update account information.

- **Marketo Measure Data Warehouse** — All data generated by Marketo Measure is stored in the Marketo Measure data warehouse, which is a Snowflake instance.

Additionally, Marketo Measure includes the following integrations:

- **CRM Integrations** — Marketo Measure integrates with CRM solutions to house and organize all the data that is captured by bizible.js. Currently, Marketo Measure has API integrations with two (2) CRM systems: Salesforce and Microsoft Dynamics. However, only one CRM integration connection can be used for each Marketo Measure instance. Once the Marketo Measure touchpoint data is in the CRM, customers can see the granular information related to each touchpoint and generate reports to understand how their channels are performing.
- **Third-Party Applications** — Because marketers rely on many different applications to run their marketing efforts, Marketo Measure is integrated with third-party marketing automation, ad platforms, A/B testing, analytics, and live chat applications. A current list of third-party applications is available on Adobe Experience League.

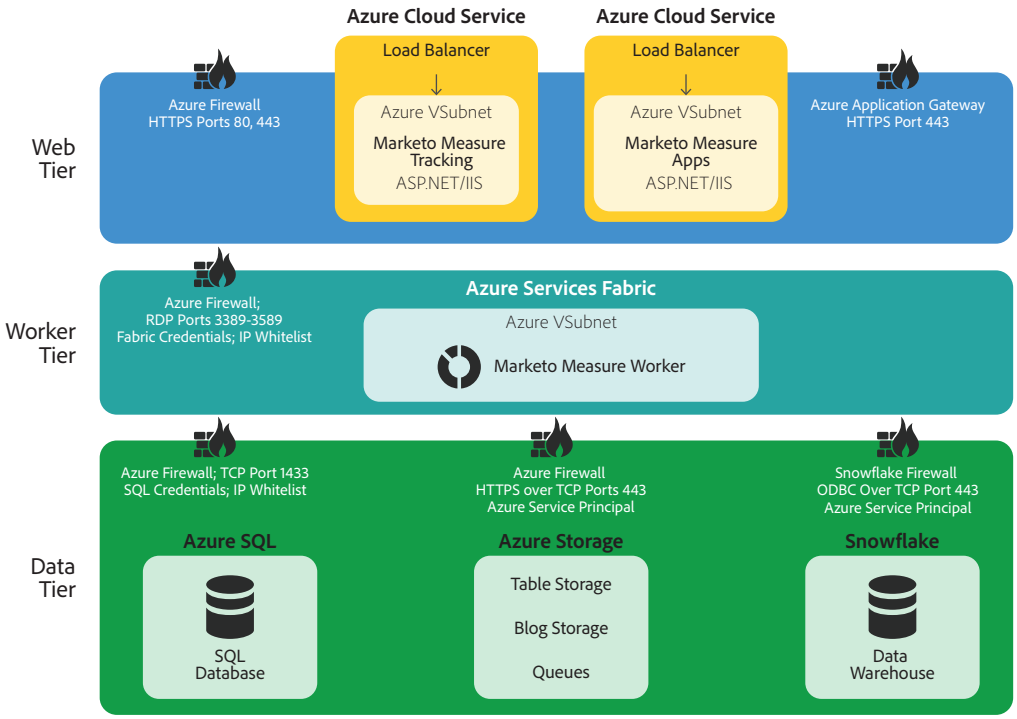

Figure 1: Marketo Measure Solution Architecture

All connections between Marketo Measure components as well as connections to external components are conducted over secure, encrypted connections, as further described below.

Security Architecture and Data Flow

The following steps describe how data flows in a Marketo Measure implementation. This section assumes that the customer has already defined the data they want to track. Step numbers correspond to Figure 2, below:

1. When a visitor lands on a customer's website with the script tag referencing bizible.js, the visitor's browser makes a request to a Content Delivery Network (CDN) server[1]. This request includes a standard set of information about the user's machine configuration and the page they are viewing as well as the pre-defined information the customer wants to track. Along with the script, the CDN server returns a cookie containing a pseudonymous visitor ID, which is included in subsequent page requests.

2. Throughout the visitor's web session, the Marketo Measure client-side code relays the tracked information to the Marketo Measure Tracking Server using HTTPS.

3. The CDN server forwards the user data to the Marketo Measure Tracking Server using HTTPS. This data is then stored in Azure Table Storage.

4. Periodically, the raw CDN logs are downloaded to Marketo Measure using SFTP. The logs are then processed, and the information is stored in Azure Table Storage (for redundancy).

5. The Marketo Measure processing platform periodically (typically every 15 minutes) queries external integrations (e.g., CRM, ad providers) for any updates since the last synchronization point.[2]

6. These updates are applied to Marketo Measure customer-specific data in the segregated client data store. (For more information on data segregation, please see the "Marketo Measure Network Management" section below)

7. The Marketo Measure processing platform updates the touchpoint and attribution data based on the configuration settings stored in the Marketo Measure product configuration database. The results are then stored in the segregated client data store.

8. Periodically, some of the data in the segregated client data store is exported into an external data warehouse (a Snowflake instance hosted in Azure East-US2).

9. If the customer has purchased the data warehouse add-on feature, they are given access to a read-only Snowflake account to access their data warehouse.

10. The customer can also access static data dashboards (implemented using Looker) to inspect their data directly using the Marketo Measure UI.

[1] Marketo Measure hosts bizible.js on Edgio EdgeCast CDN servers to ensure high performance and eliminate latency.

[2] All processing settings can be customized using the Marketo Measure UI.

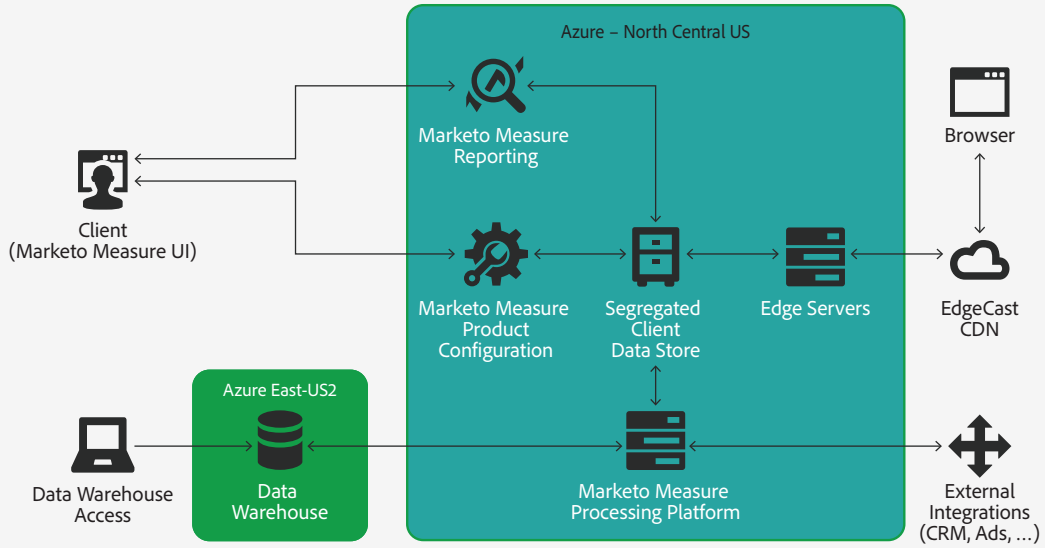

Figure 2: Marketo Measure Data Flow

Data Encryption

Marketo Measure uses HTTPS TLS v1.2 to protect data in transit. For redundancy purposes, Marketo Measure also downloads the tracking logs from the CDN using SFTP.

User Authentication

Marketo Measure supports four (4) different types of user-named licensing. You can find more information about each identity type and Adobe Identity Management Services (IMS) on the Adobe Trust Center.

Hosting Locations and Security

The Marketo Measure solution is hosted on Adobe-leased data centers managed by our trusted cloud hosting provider, Microsoft Azure, in US-North Central and US-East.

Adobe cloud service infrastructure partners maintain very strict controls around data center access, fault tolerance, environmental controls, and network security. Only approved, authorized Adobe employees, cloud service provider employees, and contractors with a legitimate, documented business need are allowed access to the secured sites.

Segregated Client Data

Each customer's data is stored in a dedicated Azure Storage Account and a dedicated Snowflake schema. The only access to these servers and databases is via secure access by the application. All other access to the application and content servers is made only by authorized Adobe personnel and is conducted via encrypted channels over secure management connections.

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.

07/24