Match My Email

Security and Privacy Policies

Cloud-Based, Automated Email Integration for Salesforce.com

Match My Email ("MME") is an Integration as a Service app. The Match My Email cloud at Amazon Web Services imports copies of emails from IMAP-compatible email systems via Transport Layer Security 1.2, processes the emails and then uploads relevant emails to Salesforce.com ("SFDC") records based on attribute-matching algorithms. MME follows industry best practices related to security and privacy to ensure data confidentiality, integrity, availability and regulatory compliance. MME models its security and privacy policies on the requirements and guidelines of the SFDC AppExchange Security Review: https://developer.salesforce.com/page/Security_Review. Each new version of the MME Service must pass the SFDC Security Review before it is put into production.

1. Application Security.

- MME has a robust software development lifecycle with security and privacy being core components.
- All developers are trained to follow secure development rules to avoid all potential security breaches such as SQL injection, Cross Site Scripting, access violation and other threats. Security training is repeated regularly.
- Source code is reviewed by a dedicated Security Engineer before being push to production.
- The application is tested for security and privacy issues with manual and automated security testing tools. There is a strict segregation of duties within the development, test and production environments. Only reviewed and tested code which complies with security specifications is deployed to production.
- Encrypted in Transport: All data and credentials (e.g., usernames, passwords, token and security strings) are encrypted in transit with Transport Layer Security 1.2 (TLS 1.2).
- Encrypted at Rest: Data and boot volumes are stored using AWS Elastic Block Store Encryption. Amazon EBS uses a data key to encrypt all disk I/O to the volume

- Copies of emails uploaded to SFDC from the MME cloud are compliant with SFDC's user permissions, profiles and role hierarchies.
- Black and grey list confidentiality controls are provided to block emails based on email address or email body tag from entering the MME cloud or being processed for upload to SFDC. Based on MME's folder selection feature, users control which email messages are synced to Salesforce and which are not.
- MME uses modern cloud authentication technologies including OAuth to connect with SFDC and API connections to G Suite and Microsoft 365.
- MME is a server-based IaaS app which does not download data to remote devices like laptops and smart phones.

2. Host/Platform Security.

- MME uses the latest version of a major Linux distribution to ensure state-of-the-art security at the operating system level on its servers. On all MME servers, unnecessary services are disabled, default accounts and passwords are removed/changed, passwords are encrypted and all users have unique usernames.
- Security patches are applied as soon as possible after they are released.
- Servers can be accessed remotely by authorized personnel only via secure connections.
- System logs are collected and regularly reviewed for security activity.
- Strong passwords are enforced.
- An enterprise-wide anti-virus solution with regular updates is implemented on all MME servers.

3. Network Security.

- Internal networks are protected with Stateful Packet Inspection Firewalls.
- Web/Application and database servers are segregated.
- No wireless in collocation facilities.

4. Physical Security.

- MME is hosted at Amazon Web Services ("AWS").

- SFDC has certified AWS as a trusted, secure, external hosting environment for ISVForce applications. SFDC also uses AWS as the hosting platform for its core application. Since 2008, SFDC has allowed third-party apps that participant in the ISVForce Program and that have passed its Security Review to be hosted on AWS. http://www.salesforce.com/company/news-press/press-releases/2008/11/081103-5.jsp
- AWS has ISO 27017 certification [see https://aws.amazon.com/compliance/iso-27017-faqs/], including physical security. Data center access is restricted to authorized personnel only. Physical access logs are maintained. Security cameras, motion detectors and alarms are implemented in the data center that are monitored on a 24/7/365 basis. Data center has implemented controls to prevent the infrastructure against external threats and hazards (fire, earthquake, flooding, etc.)
- MME only uses AWS services that are 'HIPAA Eligible', 'FERPA Eligible' and "FINRA Eligible" including Amazon Elastic Block Store (Amazon EBS), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Virtual Private Cloud (VPC) and Amazon Simple Notification Service (SNS).

5. Operational Security.

- MME networks are actively monitored with automated and manual tools. Administrators are alerted about security or performance issues.
- Disaster Recovery and Business Continuity Plans are implemented and periodically tested.
- Employee Training and Security Awareness Program are implemented and run.
- A robust change management process ensures that all changes are documented and approved.

6. Privacy Policy

- To comply with The Privacy Shield Agreement, signed by the US and EU in August 2016, RAE Internet stores email or Salesforce data related to EU customers on servers located in the European Union. RAE Internet has established an instance of MME in a European AWS data center. As of May 25, 2018, all EU customers are encouraged migrate to the EU app servers and to enter into a Data Protection Addendum to the Master Subscription Agreement to comply with General Data Protection Regulation. ("GDPR").

Data related to rest of the world customers are hosted on servers at AWS data centers in the either the EU or the United States.

- Per Salesforce guidelines, all user email and Salesforce data processed and presented by a third-party app must be private to the end-user by default and locked down under strict access and permissions control rules. MME has been architected to comply with this SFDC requirement, so all user email and Salesforce data that appears in the Email Cloud screen of the MME app, whether directly from the MME login page or through a Web Tab in Salesforce, are completely private to the end-user. Such data are stored securely so Application, Cloud and Domain Administrators do not have access to individual user content.
- For non-EU users, and only via a Privacy Waiver, signed by an authorized officer of a subscribing organization, can an individual's end-user privacy be waived in the MME Cloud. The execution of a Privacy Waiver makes individual end-user data visible to the subscribing organization's MME Cloud and Domain admins only. MME Global Application admins do not have access to user emails, Salesforce data or credentials under any scenario.

7. **Google data privacy**

- MME can be configured to scan Gmail/G Suite accounts for new emails, upload copies of the emails to the MME cloud and store them on MME's servers at AWS for up to 45 days for further processing.
- By analyzing attributes and content of emails (for example full email addresses, word(s) in Subject Line and structured body tags), MME matches emails to records in the user's Salesforce account and then uploads email content to the data store in the Salesforce cloud.
- MME is configured by default to upload email attachments to Salesforce's Notes and Attachments store. That configuration can be changed by a Cloud Admin.
- Emails and their associated credentials are encrypted in transport from the Gmail cloud to the MME cloud and then to the Salesforce cloud using TLS 1.2.
- Authentication to the Gmail cloud is via server-to-server OAuth 2.0 flow as specified by Google: https://developers.google.com/identity/protocols/OAuth2ServiceAccount.

To access Gmail data, MME uses Admin API, Directory API, Gmail API. Alternatively, cloud admin can choose authentication via username and application/user password.

- OAuth and IMAP credentials are encrypted in storage in the MME cloud with strong AES 256-bit encryption; MME operations personnel do not have access to user content or credentials.
- A user is provided with a private view of emails uploaded to the MME cloud.
- Email read/write/delete functions in Salesforce are governed by Salesforce roles, permissions and profiles.
- Email views are private by default, however, they may be shared with other members of the user's organization upon request from an authorized officer of the user's organization.
- MME stores email address, Google User Id, name, username and OAuth tokens of a user on its servers using Amazon EBS with Encryption and uses this data for authentication.
- MME uses a user's email address to send emails related to service operation such as service interruption alerts.
- Data may be written to a system log and stored on MME's servers for six months for troubleshooting purposes: email address, Google User ID, username, email message ID and size, folder ID and name.
- MME does not share Google data with third parties.

8. Microsoft 365 data privacy

- Emails and their associated credentials are encrypted in transport from the Microsoft 365 cloud to the MME cloud and then to the Salesforce cloud using TLS 1.2.
- Authentication to the Microsoft 365 cloud is via Microsoft identity platform and the OAuth 2.0 client credentials flow https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-client-creds-grant-flow . To access Microsoft 365 data MME uses Microsoft Graph API, Office 365 API, Microsoft EWS. Alternatively, cloud admin can choose authentication via username and password and IMAP protocol to access Microsoft 365 data.

- OAuth and IMAP credentials are encrypted in storage in the MME cloud with strong AES 256-bit encryption; MME operations personnel do not have access to user content or credentials.

9. HIPAA Compliance

- The management of RAE Internet Inc. has reviewed the "Security Standards for the Protection of Electronic Protected Health Information," found at 45 CFR Part 160 and Part 164, Subparts A and C, commonly known as the Security Rule, of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). RAE Internet's management believes that Match My Email conforms with the technical safeguard standards of HIPAA as they pertain to Access Control, Automatic Logoff, Audit Controls, Person or Entity Authentication and Transmission Security and Encryption.

10. FINRA Compliance

- The management of RAE Internet Inc has reviewed Rule 30 of Regulation S-P (referred to as the "Safeguard Rule") requires firms to establish written procedures reasonably designed to "(a) insure the security and confidentiality of customer records and information; (b) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (c) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer." The management of RAE Internet believes that Match My Email conforms to Rule 30.

11. FERPA Compliance

- The management of RAE Internet Inc has reviewed the data security and privacy requirement of the Family Educational Rights and Privacy Act (FERPA) and believes that the Match My Email cloud-based email integration application for Salesforce.com is compliant.

Attestation by Officer of Corporation: Paul Sterne, President, RAE Internet Inc., June 2020