Email Meter
Security Handbook

What is Email Meter?

Email Meter is an email analytics solution providing employee performance and productivity metrics.

Our Commitment to Security

As your email inbox contains exceptionally sensitive and important information, the security of your data lies at the very heart of how we create and deliver Email Meter.

Our company, ShuttleCloud, manages Gmail and Google Contacts' data importing service. This has given us years of experience handling sensitive data securely — we are held to incredibly high standards for security, and without stringent security and privacy policies, Email Meter would not exist.

ISO 27001

Email Meter is ISO 27001 certified, and has developed an ISMS that is also adequate to SOC 2 Type 2 standards. View the certificate here.

GDPR.EU

Email Meter is fully compliant with GDPR & CCPA. We also strive for compliance in EU/US data regulations, such as Standard Contract Clauses.

Email Meter is verified yearly by Google, with a rigorous audit conducted by a third party. This includes pentests, deployment reviews and policy and procedure reviews.

Infrastructure

- Email Meter is hosted on Google Cloud Platform (GCP) which is highly scalable, secure, and reliable. More info here.
- Customers can choose which geographic location hosts their data.
- The GCP data centers are physically protected 24/7, and use top surveillance to monitor any suspicious activity.
- Data is backed up automatically by GCP every few hours. Email Meter performs additional backups in encrypted state.
- Email Meter benefits from managed DDoS protection which safeguards all applications running on GCP.

Data Privacy

- All data in transit is encrypted using the latest recommended secure cipher protocols, including TLS 1.3.
- Data at rest in Email Meter’s production network is encrypted using AES-256, which is managed by GCP.
- All API and client communication require HTTPS connections.
- All customer data is segregated, with unique Google BigQuery databases.
- Email Meter has security monitoring technology in place to detect incidents, and processes to quickly resolve them.

Internal Security

- All employees go through background checks prior to employment, always within the limits of applicable labor law.
- All employees undergo general security training as part of their onboarding. Engineers need to pass additional training before gaining access to production systems.
- All employees sign a Confidentiality Agreement, outlining their responsibility in protecting customer data.
- All sensitive data is handled through our extensive ISMS to minimize risks.
- Email Meter has a defined framework to detect and quickly respond to security incidents and maintain service continuity.

Other Security Controls

- Application source code is stored in a secure environment and changes go through at least two review processes.
- Email Meter has dedicated staging environments for development, separate from production, which use dummy or internal data and doesn’t have access to any customer data.
- Access to sensitive data is restricted to a small number of designated employees, using Google Cloud Platform IAM for authentication.
- Email Meter has a Vulnerability Disclosure Program where we encourage security researchers to report security vulnerabilities.

Google Workspace Access and Authentication

Email Meter access and authentication can be fully controlled through Google Workspace, so you can use all inbuilt security & control features.

Email Meter never has access to the body or attachment of your emails. We use the **minimum necessary scopes**: Gmail Metadata.

Email Meter uses the Google OAuth 2.0 protocol to authenticate users. **We don't handle any password or login information**, and OAuth Tokens are encrypted before being stored.

Administrators can enable **multi-factor authentication** via Google Workspace. This includes: security keys, Google prompt, multifactor application, text message, phone call...

If you have **SSO** enabled in Google Workspace, you'll be able to use it to authenticate in Email Meter. Users can use any **SAML2** identity provider available in Google Workspace.

A **domain-wide centralized installation** is available through the Google Workspace Marketplace. This puts admins under full control.

Organizations can **revoke Email Meter access** totally or partially anytime through their Google Workspace admin dashboard.

Frequently Asked Questions

What email data can Email Meter access?

We never process or store the body or attachments of your emails because we don’t have access to them. The only information that we analyze are the headers which contain data such as: from, to, subject, label or date. This is possible because we use the minimum necessary scopes: Gmail Metadata.

Is my data secure and encrypted?

Yes, your data is encrypted both in transit (TLS 1.3) and at rest (AES-256). It never leaves the Google Cloud. The process to ingest email data and turn it into statistics happens entirely inside Google Cloud Platform, and almost every step of the process is serverless. That means you benefit from Google’s huge investment in security: they’re in charge of everything, including encryption.

Where is my data stored?

Email Meter is built entirely on top of Google Cloud Platform. This enables us to leverage all of Google's investments in data centers around the world. By default, all of our data is hosted in the EU, but you may choose to have your data stored in a different region of your choice.

Does Email Meter support multifactor authentication?

Email Meter uses a Google Account for authentication, so this means it will use whatever multi-factor authentication is allowed in Google Workspace and configured by the user. This includes, but is not limited to: SMS, Google Prompt, multi-factor application, security keys, backup codes... We strongly discourage the usage of SMS as an option for MFA.

Frequently Asked Questions

Are you GDPR compliant?

We are fully compliant with all GDPR regulations and provide full rights to our users, including deletion of data and access to the list of subprocessors that Email Meter uses.

Can I stop Email Meter from accessing my data at any time?

Yes, you can check what data we do have access to, and revoke our access to that data, at any time. Organizations can revoke Email Meter access to their Google Workspace account anytime through their Admin Dashboard if Email Meter was installed domain-wide.

What happens with my data if I leave?

Email Meter will delete any company's data once an explicit request is submitted and the requester's identification is properly validated. All deletion requests will be completed immediately, but as described in the privacy policy, we retain some system logs for 30 days, and audit logs for 400 days. The customer's own data and customer related data will be completely purged from any backup after 3 months.

Who are Email Meter's technology providers?

Email Meter is built entirely on top of Google Cloud: our system's architecture is built entirely on Google Cloud Platform, the data is extracted from Gmail, and the user security controls are handled through Google Workspace.

Frequently Asked Questions

What are your backup and disaster recovery processes?

We have automatic multi-region backups, managed directly via Google Cloud Platform. In case of disaster we can quickly recover the data of these copies, as described in our data recovery policy and here.

Where can I find out more about Email Meter's security resources?

Terms of Service: https://www.emailmeter.com/terms-of-service

Privacy Policy: https://www.emailmeter.com/privacy-policy

Security Page: https://www.emailmeter.com/safe

If you have any more questions or concerns reach out to your point of contact or hello@emailmeter.com