mailtrack.io

Last update: 11 may 2023

Security Whitepaper

Introduction

In Mailtrack we take information security very seriously. We have invested a great deal of time, effort and resources to ensure that our users' information is secure.

1. Compliance

Every app that requests access to restricted scope Google user's data is required to go through a yearly security assessment. This assessment helps keep Google users' data safe by verifying that all apps that access Google user data demonstrate capability in handling data securely and deleting user data upon user request. This security assessment is based on OWASP Security Verification Standards and uses cloud application security assessment framework (CASA).

We enforce as well Google's API Services User Data Policy which is required for all apps that access Google APIs.

We meet as well all requirements of the General Data Protection Regulation (GDPR). You can check all details in our public privacy policy

2. Internal policies and procedures

In Mailtrack we enforce policies an procedures that reduces risks and provides adequate response to security incidents. Such include:

- An internal information security policy that ensure that all users comply with rules and guidelines related to the security of the information stored digitally at any point in the network
- An internal risk management policy that identifies, reduce and prevents undesirable incidents or outcomes
- An internal incidence response plan that establishes roles, responsibilities and actions when an incident occurs. We walk through this procedure at least once a year.
- A procedure to report app or service data breaches to supervisory authorities and individuals affected by the breach within 72 hours of detection.
- An a public Vulnerability Disclosure Program that provides means for external parties to report vulnerabilities.
- Upon requesting via privacy@mailtrack.io, we can provide you with our Information Security Policy

3. Secure development

All employees receive a security training as part of the onboarding process. All development staff receive as well a yearly secure coding training that include topics such as OWASP Top 10 or related.

We are using static analysis tool sonarCube and other static analysis tools to detect security issues on the code prior deploying it to production.

We have as well a Code Review Policy that enforces a check of our Secure Development Policy within the peer review.

No production data leaves production environment and developers use their own datasets while developing new functionalities. We enforce multi-factor authentication (MFA) for all administrative or developer access to the deployment environment and other supporting tools such as version control system or Gsuite.

4. **Security of users data**

Mailtrack does not maintain any of its own physical datacenters, nor is any production data or customer data stored on local media. Instead, all production data is stored and processed in a virtual private cloud (VPC) in SOC 1 Type II, SOC 2 Type II, and ISO 27001 certified datacenters hosted by Amazon Web Services (AWS).

Customer data is hosted and processed by our cloud-based database and analytics providers, which, themselves, use public cloud infrastructure providers such as AWS, Google Cloud Platform (GCP) to host their environments.

Network Security

We enforce network hosting all environments in a Virtual Private Cloud in Amazon Web Services, containing separate public and private subnets. No inbound internet traffic is allowed to the private subnets and all application servers only reside in private subnets without public IP addresses. Only Amazon managed and maintained load balancers have ingress access to the application servers. Production access is restricted using VPN software.

Firewall protection

Mailtrack servers are protected by a firewall (Amazon WAF) which rules are periodically reviewed and updated by our security team.

Data Encryption

All user data is either encrypted in transit or at rest.

Https is enforced to all users reaching our website and all data is transferred encrypted in transit with TLS 1.2 for all communication between Mailtrack servers and third parties.

mailtrack.io

User data is encrypted at rest ins AWS services such as OpenSearch, RDS and S3. When using Mailtrack, all your data is encrypted using Server-side encryption with Amazon S3 managed keys (AWS KMS) that uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.

All production secrets and keys are managed and stored encrypted using Vault.

Security updates in production environment

Our production Webservers and worker machines that provide Mailtrack functionality are built from scratch in every deploy, what is called inmutable infrastructure, and the images we use to build this machines are patched on every deploy.

User authentication

All user authentication to access Mailtrack is handled by Google, which allows two factor authentication if enabled.

The Mailtrack team