Gtmhub

IT & Security FAQ

This document provides an overview of Security and IT measures implemented to protect Gtmhub's SaaS platform.

October 2021

Security Management & Compliance

Is Gtmhub compliant with any industry-recognized security framework?

Gtmhub has been validated against the SOC 2 Type 2 framework by an independent third-party auditor. On our web site you can find a public version of the SOC 2 report, known as SOC 3, which is available for instant download.

Gtmhub is also a certified with the ISO 27001 standard. Our policies, procedures and processes are aligned with the ISO framework to ensure stringent security controls are in place. The ISO 27001 certificate is available on our web site.

Is Gtmhub compliant with GDPR?

Yes. Our Data Processing Agreement (DPA) defines our responsibilities as a Data Processor and provides information on Gtmhub practices for data protection.

Where can I find Gtmhub's data privacy policy?

Privacy and Security policies can be found on our Help Portal through the following links - privacy and security.

Where can I find the list of Gtmhub sub-processors?

All Gtmhub sub-processors undergo a thorough security vetting process. Evidence of that can be found in our SOC 2 report. For a complete list of sub-processors please visit the GDPR info page.

Technical Questions

Where do we store client data?

Clients can choose between the following data centers to host their application instance:

- EU data center in Netherlands.
- US data center in Washington.

Both are managed by Microsoft Azure and are ISO 27001, ISO 22301, SOC 2 and PCI-DSS compliant facilities.

Who has access to client data?

Access to data in Gtmhub is given on a 'need-to-know' basis. By default, Gtmhub employees do not have access to client data, but to ensure the smooth operation of Gtmhub's platform certain employees need to perform maintenance activities. For example, installing security patches or diagnosing service outages.

Note that client data is never processed on Gtmhub employee workstations or on-prem servers in the office, it resides only on Azure Cloud systems.

What technologies did we use to build the Gtmhub application?

Gtmhub is built upon multi-tier microservices architecture based on Kubernetes containers. Our application code is developed in-house and is written in Java and Go programming languages.

How do we protect client data stored on Gtmhub systems (data encryption)?

Client data stored on Gtmhub systems is protected by AES 256 which is a military-grade encryption algorithm.

How do we ensure protection of data transfers over the Internet?

The data flow between client endpoints and Gtmhub occurs over TLS 1.2 & 1.3 encrypted connections which provide server authentication and data encryption. Data is never exchanged in cleartext.

Do you support different roles and permissions on your platform?

The platform has a built-in Role-Based Access Control (RBAC). Client accounts with administrator privileges have the ability to assign permissions on a granular level for each user or group. More information can be found in this article.

How do you protect your platform from malicious attacks? (Firewall, WAF, DDOS protection.)

Gtmhub applies “defense in depth” strategy to protect its systems. That includes filtering of the Internet traffic by using network firewalls, Web Application Firewalls (WAF) and managed DDoS protection.

Can we limit access to client data to a specific set of IPs?

Yes. Customers can provide a list of IPs which can be allowed access to their Gtmhub application instance. All other IPs will be blocked from accessing the service.

Do we keep backups of client data and how are they protected?

Yes, we make full data backups every 10 minutes. Backups are stored in a different region while preserving data residency and encryption requirements. More information is available in our SOC 2 report.

Does Gtmhub support Single Sign-On (SSO)?

Yes. Clients can use their existing SSO provider for authentication to Gtmhub. Some examples include Azure AD, Okta, Google or on-prem Active Directory. Basically, any system that supports SAML 2.0 or OpenID Connect (OIDC) protocols can be linked with Gtmhub for authentication.

Can we onboard employees automatically via the SSO provider?

Yes. Once SSO is configured for your Gtmhub account there will be no need to invite every employee manually. You can enroll everyone, specific group or an individual, to access Gtmhub application automatically using Just-in-Time (JIT) provisioning.

Can clients control the access to Gtmhub via their SSO provider?

Yes. Once the SSO is enabled the access to Gtmhub application will be controlled by your Identity Provider. When SSO is enabled for your account the traditional username and password authentication will be disabled.

What are the sign-in options if we do not have Identity Provider to leverage the SSO functionality?

In this case you can invite users by e-mail. For mass onboarding a list of users can be imported in CSV or Excel format onto the platform. Users will receive an e-mail invitation and will be required to authenticate by the traditional method with a username and password.

Can we use multi-factor authentication for sign-in to Gtmhub?

Multi-factor authentication can be used if SSO is enabled, and if client's Identity Provider supports the feature. This way the MFA settings will be managed on the client's side.

Can we make bulk OKR upload from a spreadsheet/CSV file?

It is possible to bulk upload OKRs from a spreadsheet. Note that this feature is not visible inside the end-user interface and you need to contact our Support team.

Security Testing

How is the security of Gtmhub web application tested?

Gtmhub web application undergoes daily vulnerability scans performed by automated security tools to uncover potential flaws or misconfigurations. All findings are assessed and remediated according to our internal vulnerability management procedure.

Do you conduct regular Penetration Testing of your application?

We have hired an external company specialized in Penetration Testing to conduct an assessment of our platform. Testing is performed annually or on a significant change in our architecture.

Do you allow customers to undertake their own security testing?

Yes, we allow clients to undertake their own security testing but these must be requested in writing and approved by security@gtmhub.com. Note that denial-of-service (DOS) tests are not allowed.

Credit Card Data Security

How do we process credit card data?

The only place where credit card information might be collected is when customers pay for their subscription through our web site. In this case the credit card information is securely passed to our payment gateway (Braintree) and is not stored at Gtmhub. We do not collect credit card information from end users.

Gtmhub Reports and Documentation

Would you provide your SOC 2 report for review?

Yes, the report is available for download at https://gtmhub.com/security.

Would you provide your ISO 27001 certificate?

Yes, the certification is available for download at https://gtmhub.com/security.

Does Gtmhub share its penetration testing reports?

Yes, the Penetration Testing report is available for download at https://gtmhub.com/security.

Will Gtmhub fill out customer security questionnaire?

Before sending your questionnaire please make sure you have reviewed our SOC 2 Type 2 report which might already have answers to some of your questions.

For additional information please contact your Account Executive.