



Bubbi Security Whitepaper

Bubbi Technical Documentation · Version 2.0 · © 2025 Bubbi. All Rights Reserved.

Bubbi Pixel and Behavioral Module Security



Bubbi's solution consists of two main components that together enable behavioral tracking and personalized content delivery:

1. **The Tracking Pixel**, a lightweight JavaScript for user and session-level behavior tracking.
2. **Behavioral Influence Modules**, interactive components rendered to the user with the purpose of influencing behavior in real time.

The Bubbi Tracking Pixel is a JavaScript snippet customized for each customer site. It can be implemented directly on the customer's server or through services such as Google Tag Manager (GTM) and hosted either by the customer or by Bubbi's Google Cloud Platform (GCP) environment.

The Pixel collects and processes behavioral data and connects this to a unique, pseudonymized user and session identifier stored in a cookie. When a visitor reaches a part of the site where a Behavioral Module may be displayed, the Pixel sends a secure request to a Bubbi API endpoint (GCP-hosted). This request contains the anonymized user and session ID. The endpoint responds in real time, indicating whether a module should be displayed, and may also include parameters such as text variations or configuration details.

All communication between the Pixel and Bubbi Services occurs over TLS-encrypted outbound requests, ensuring no inbound connections are initiated from Bubbi's systems to the customer site.

For more detailed information about Bubbi Pixel and Site Security, please contact Bubbi.

Deployment Models



Bubbi supports two architectural deployment models to fit different customer requirements:

1. Unified Model (Tracking and Modules Combined)

In this configuration, both the tracking functionality and the Behavioral Modules are included within the same JavaScript Pixel.

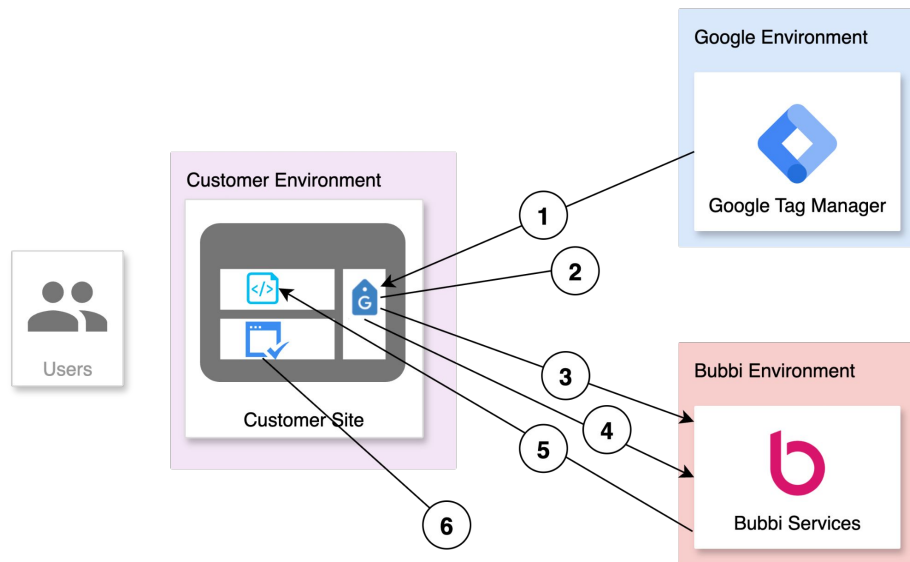
- Suitable for proof-of-concept implementations or rapid deployment.
- Simplifies setup and iteration during early testing.
- Typically hosted and managed by Bubbi via GCP and implemented through GTM.

2. Separated Model (Independent Tracking and Modules)

In this configuration, the tracking is managed by a standalone Bubbi Pixel while the Behavioral Modules are developed and hosted separately - either on the customer's infrastructure or Bubbi's GCP environment.

- Preferred for customers with stricter security or scalability requirements.
- Reduces dependency between tracking and module delivery.
- Allows the customer to maintain full control of hosting, access, and monitoring.

Client Side Architecture



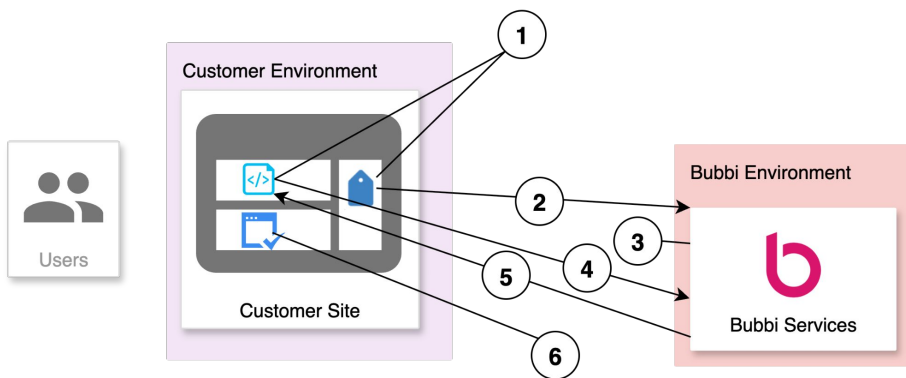
When the Bubbi Pixel is implemented through Google Tag Manager or similar tools, both the Pixel and optional modules are delivered dynamically to the customer site.

The process flow is as follows:

1. The Customer Site loads the Bubbi Pixel JavaScript.
2. The Pixel begins tracking user behavior and session data.
3. Tracking data is sent to Bubbi Services for analysis and prediction.
4. The Pixel requests a decision from Bubbi's API regarding module display.
5. Bubbi Services respond with module instructions and parameters.
6. The content is rendered to the visitor.

This loop repeats continuously throughout the session to adapt to real-time behavior changes.

Server Side Architecture



For server-side configurations, the Bubbi Tracking Pixel operates client-side while the Behavioral Influence Modules are hosted on the customer's infrastructure or within Bubbi's Google Cloud Platform (GCP) environment.

1. The Customer Site loads the Bubbi Tracking Pixel JavaScript.
2. The Pixel collects behavioral data locally and transmits it securely to Bubbi Services.
3. Bubbi Services analyze the data and generate predictions.
4. The Customer Site requests a decision from Bubbi's API regarding module display.
5. The API response specifies whether a module should be displayed and, if so, which version or content variant.
6. The server renders or injects the module into the page before or during runtime.

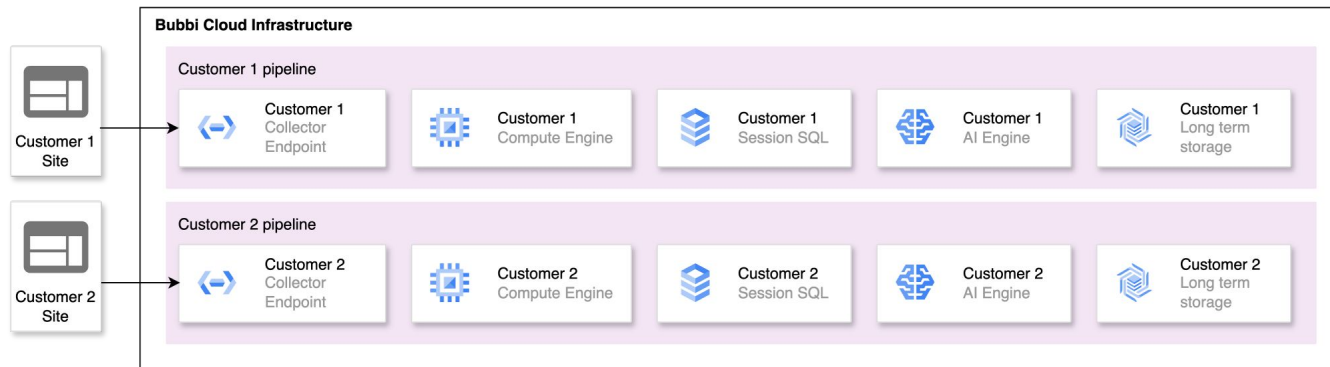
This setup enables minimal latency and allows the customer to retain full control over caching, load balancing, and content delivery. Hosting modules server-side also reduces the client's attack surface and allows for tighter integration with existing backend systems or CDNs.

In server-side configurations, it can also be advantageous to load the Bubbi Tracking Pixel as a first-party script, hosted directly on the customer's domain. Doing so strengthens data ownership and compliance, improves tracking reliability, and minimizes the risk of third-party script blocking by browsers or privacy filters, while maintaining the same secure outbound communication pattern via TLS.

Customer Data Separation



The Bubbi services are built based on an architecture that inherently guarantees full separation of different customer's data. Each customer onboarded to the service gets its own, logically separated, pipeline of service components where the customer's data is processed and stored.



Data from each customer is only processed and stored within the customer specific service pipeline. All training of the AI model for a customer is done within the customer pipeline and only on the data pertaining to the customer. For more detailed information about customer separation, please contact Bubbi.

Data encryption



All data processed within the Bubbi services is encrypted both in transit and at rest using modern and approved encryption algorithms. The network connection between a customer's Bubbi Pixel and the Bubbi Collector Endpoint for that customer is secured through specific TLS certificates for each endpoint. The certificates are managed through the Bubbi Cloud Infrastructure.

Data is encrypted at rest using built-in capabilities within the Bubbi Cloud Infrastructure provided by Google Cloud Platform (GCP).

More detailed information regarding encryption in GCP can be found here:

<https://cloud.google.com/docs/security/encryption/default-encryption>

Privilege Access Management



All access to the Bubbi Cloud Infrastructure is considered privileged and treated that way. Only authorized Bubbi personnel have access to the infrastructure and the services therein and all access is granted based on the principle of least privilege. That means that even authorized Bubbi personnel only have access to the parts of the infrastructure needed for their role. All privileged access to the Bubbi Cloud Infrastructure requires the administrator to authenticate using approved multi-factor authentication (MFA).

The roles at Bubbi with access to the infrastructure includes:

- Global administrators
- Infrastructure administrators
- Architects
- Service developers
- Security engineers
- Quality assurance engineers

The Bubbi Cloud Infrastructure is provided by Google. No service provider personnel have access to the data within the Bubbi Cloud Infrastructure without the explicit approval from Bubbi. More information about how Google provides their customers control over the access to their data within the Google Cloud Platform (GCP) can be found in the Google Cloud Trust Whitepaper:

https://services.google.com/fh/files/misc/072022_google_cloud_trust_whitepaper.pdf

Customer Access to Bubbi Services



Customer users interact with the Bubbi service exclusively through the Bubbi Dashboard, where statistics and key performance indicators related to the customer's use of the service are presented. The Dashboard is the only interface exposed to customer users and does not provide direct access to the underlying infrastructure.

Access to the Bubbi Dashboard is managed by Bubbi. User accounts are created manually by authorized Bubbi personnel based on customer request, ensuring controlled onboarding and adherence to the principle of least privilege.

The primary authentication method for customer users is username and password. For customers utilizing Google-based platforms, Single Sign-On (SSO) can be enabled, allowing users to authenticate through their existing organizational identity provider.

Backup and restore



All customer data that is stored within the Bubbi services is backed up regularly. Data is permanently stored in Big Query (BQ) within the Google Cloud Platform (GCP) and is backed up using built in Time travel functionality. The data can be restored to any timestamp within the previous 7 days.

Each customer's data is logically separated at storage within BQ and is thereby backed up separately as well. Data can be restored for each customer separately or for the entire service at once if needed. The time to restore is approximately 15 minutes. The backups are stored within the GCP and only the Global Administrators at Bubbi have access to them. The Bubbi Cloud Infrastructure is provided by Google. No service provider personnel have access to the data within the Bubbi Cloud Infrastructure without the explicit approval from Bubbi.

More information about how Google provides their customers control over the access to their data within the Google Cloud Platform (GCP) can be found in the Google Cloud Trust Whitepaper:

https://services.google.com/fh/files/misc/072022_google_cloud_trust_whitepaper.pdf

More information about the Time travel backup and restore functionality can be found within the Big Query documentation:

<https://cloud.google.com/bigquery/docs/time-travel>

Security and compliance contact points



There are multiple ways to get in contact with Bubbi regarding security or compliance related questions or issues.

- Regarding preparedness and communication related to incidents, please contact alerts@bubbi.ai that is monitored and handled weekdays 08:00-18:00 CET with 30 minutes response time.
- For questions regarding the content of this whitepaper or other security related questions please contact security@bubbi.ai.
- For questions regarding compliance and privacy please contact privacy@bubbi.ai.