bloomreach

Bloomreach Security Whitepaper

Contents

Bloomreach as Your IT and Security Partner

Bloomreach as Your IT and Security Partner

At Bloomreach, we pride ourselves on our ability to provide our users with the tools and access they need to convert their customer information into actionable data to deliver exceptional personalized experiences. However, it is equally important that our data and information technology teams are kept up to date and equipped with the highest security measures in place to ensure the integrity and privacy of every piece of data that passes in and out of the Bloomreach application.

This whitepaper provides a detailed description of the security procedures, defense, and in-depth strategies that are instituted by Bloomreach to protect the Bloomreach Engagement product and all associated data.

Bloomreach Security Certificates

At Bloomreach, we have taken GDPR very seriously and understand the risks as well as the opportunities. We set out to become one of the first companies ever to get the Certificate of GDPR Conformity, accomplishing our mission as a pioneer. Being ISO 27017 & ISO 27018 certified, Bloomreach works together with co-authors of GDPR standards to better ensure your company's protection. And it doesn't end here, as we continue to place further emphasis on data privacy security.

We currently have the following certifications:

- GDPR 3101
- ISO 9001
- ISO 27001
- ISO 27017
- ISO 27018
- ISO 2230

Service Availability Assurance

Bloomreach Engagement is using Google Cloud Platform as a 3rd-party vendor, which runs in a multi-tenant, geographically distributed environment to support the availability of services through the use of redundant architecture. It is guaranteed by the vendor that data is distributed among a shared infrastructure through a distributed file system designed to store extremely large amounts of data across many servers.

A redundant architecture exists to ensure that data is replicated in real time to at least two geographically dispersed data centers. The data centers are connected through multiple encrypted network links and interfaces. This provides high availability by dynamic load balancing across those sites. Google Cloud Platform uses a dashboard that provides details such as resource footprint, central processing unit capacity, and random-access memory availability to monitor resource availability across their data centers and to validate that data has been replicated to more than one location.

As Bloomreach Engagement utilizes an Infrastructure as Code (IaC), the whole infrastructure can be rebuilt and recovered to the previous working state. Also, any change can be reverted back if necessary.

These recovery capabilities are periodically tested to ensure everything is functioning as expected. We test the recovery of all components at least once per year or after any significant change in a particular component

Data Location

Bloomreach operates in the Google Cloud Platform to allow for the use of our platform and tools wherever you are. Our primary data centers are located in Europe. For those who require geographically compliant server locations, we also have data centers located in the United States, Canada, and the United Kingdom. Below is the list countries and states that our servers are hosted in:

Full-system backups are performed daily using an automated system. Backups of all data are performed regularly following Bloomreach Engagement backup processes. We maintain multiple on-call independent support teams to assist employees and you with addressing incidents or potential breaches. All incidents are logged in an incident management tool and this information is distributed automatically to internal stakeholders.

Data Protection

Whenever we store data, there are several layers of encryption. By default, data is encrypted both at rest and in transit. To encrypt data at rest, the Advanced Encryption Standard (AES) is used.

Encryption at rest protects your data from a system compromise or data exfiltration by encrypting data while stored. Our encryption utilizes encryption keys, which are managed by Google.

Encryption in transit protects your data if communications are intercepted while data moves between your site and the cloud provider.

This protection is achieved by encrypting the data before transmission, authenticating the endpoints, then decrypting and verifying the data on arrival. This level of security is achieved through Transport Layer Security (TLS) to encrypt data in transit. TLS acts as a tunnel to separate data from the outside environment, and the endpoints are exchange encryption keys. GCP also encrypts and authenticates all data in transit at one or more network layers, when data moves outside physical boundaries not controlled by or on behalf of Google.

Furthermore, data in transit inside a physical boundary controlled by or on behalf of Google is generally authenticated but not necessarily encrypted. Our encryption utilizes encryption keys, which are managed by Google.

Service Risk Management

Service Risk Management

Bloomreach is hosted in GCP. We therefore share data responsibilities and potential risks between ourselves, Google, and our clients. These include external and internal risks such as human error, malicious attacks, unexpected downtimes, and unauthorized access. For each of these risks, Google and Bloomreach have taken precautionary measures to prevent harm to our customers.

Disaster Recovery

Bloomreach Engagement has implemented a disaster recovery plan to prevent data loss and ensure quick recovery in case of hardware failure, natural disasters, or other catastrophes. Bloomreach Engagement's architecture setup strives to minimize any possible interruption. This is mostly ensured by all of its components being redundant and located in separate zones.

As additional prevention, we also have a disaster recovery program. We test recovery components periodically and after any significant change in a particular component.

Incident Management

We have an incident management process in place that has been designed to identify, confine, monitor, and communicate incidents. If an incident occurs, the incident is identified, reported, and prioritized for resolution between our Support and Security teams.

Our clients are provided with the required information to be able to promptly report to their local authorities, if necessary (especially in the case of security incidents).

Bloomreach Engagement has multiple systems to ensure our production environment is running without any issues. Our highly available monitoring infrastructure continuously monitors data processing pipelines, application performance, resource exhaustion, and availability.

Bloomreach Instances

Bloomreach Instances

Bloomreach Engagement offers three main types of instances: multitenant, signle tentant and exclusive. Each instance contains different features and configurations of data layers, which we will explain below. In each of these instances, data is separated and access management is enabled to ensure your security.

Multitenant and Single tenant Instances

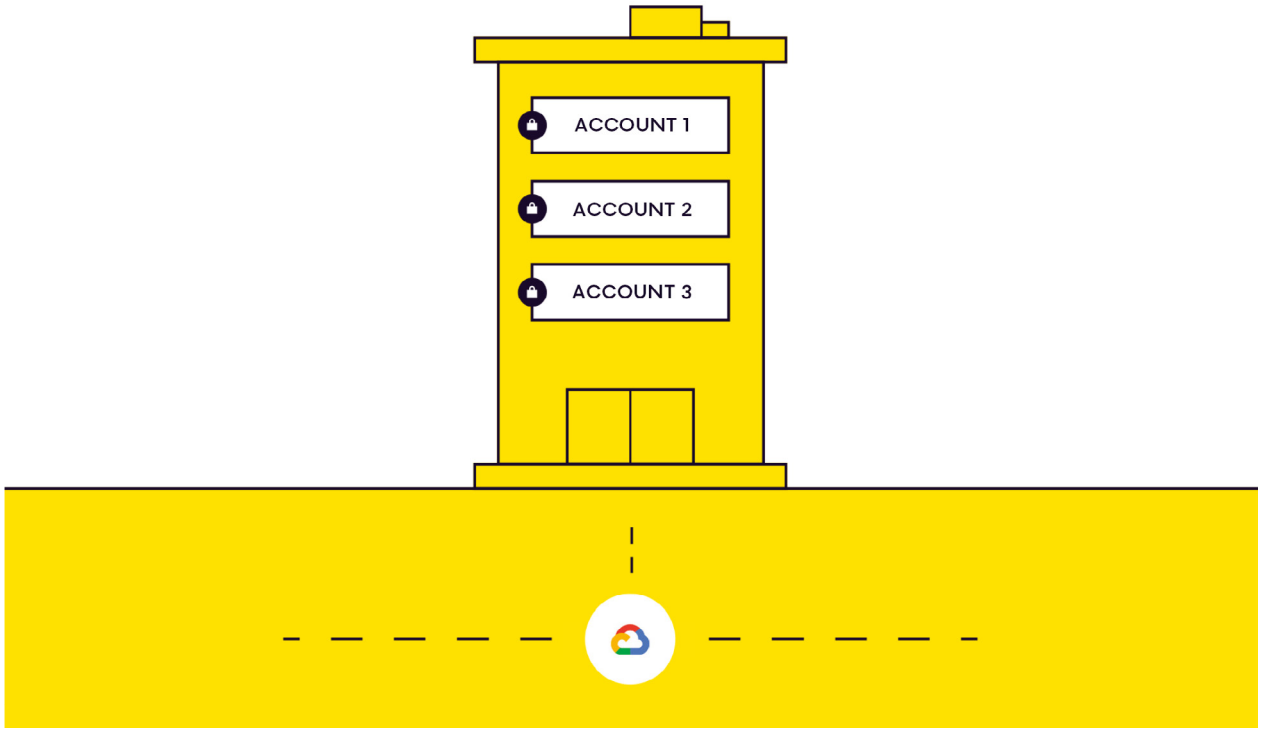
Multi and single tenant instances are data hosting service types where multiple accounts exist on one server. These instances are like an office building with separate companies (tenants) located on each floor. In this example, the building is the hosting server and the floors are the separated instances where each company occupies a designated space with their individual data. With this instance type, each account and its corresponding data is separated and kept secure while sharing the common computing capacity and security protocols of the hosting server.

Each account's data is separated and protected to prevent the other accounts from accessing it, while sharing the resources to compute the data, thus lowering the cost burden for all accounts hosted within the instance.

Multitenant Instance

The multitenant instance is like a building with multiple offices, each with a security door. All clients share a single Google Cloud Platform, but they all have different accounts, each with a separate password. Data segregation exists between multiple projects (aka offices).

Multitenant instances are typically suited for small-to-medium enterprises (SMEs) who are not subject to the strictest regulation.



Within our multitenant instance, users cannot access data from other clients, and data is separated on a front-end level. Resources are also shared on a back-end level.

Multitenant instances are encrypted at the level of GCP infrastructure and undergo periodic security scans and pen tests.

To access the account on the multitenant instance, users must choose a strong password and may use two-factor authentication (2FA) to sign in. The accounts are further secured by Captcha to fend off bot attacks. The admin of the particular project can also specify in the access management

which users can see PII (personally identifiable information) of their customers. This segregation is on the front end and back end. It also supports Single Sign-On (SSO) to meet security standards in this industry.

Multitenant Instance Features

Computing Power: Shared

Features included in our multitenant instances are:

- Password Guardian
- Captcha
- Identity Access Management (IAM)
- DDoS protection
- Firewall
- Data Encryption (SSL/TLS/AES)
- Static IPs (Shared Proxy)
- SSH Tunnel

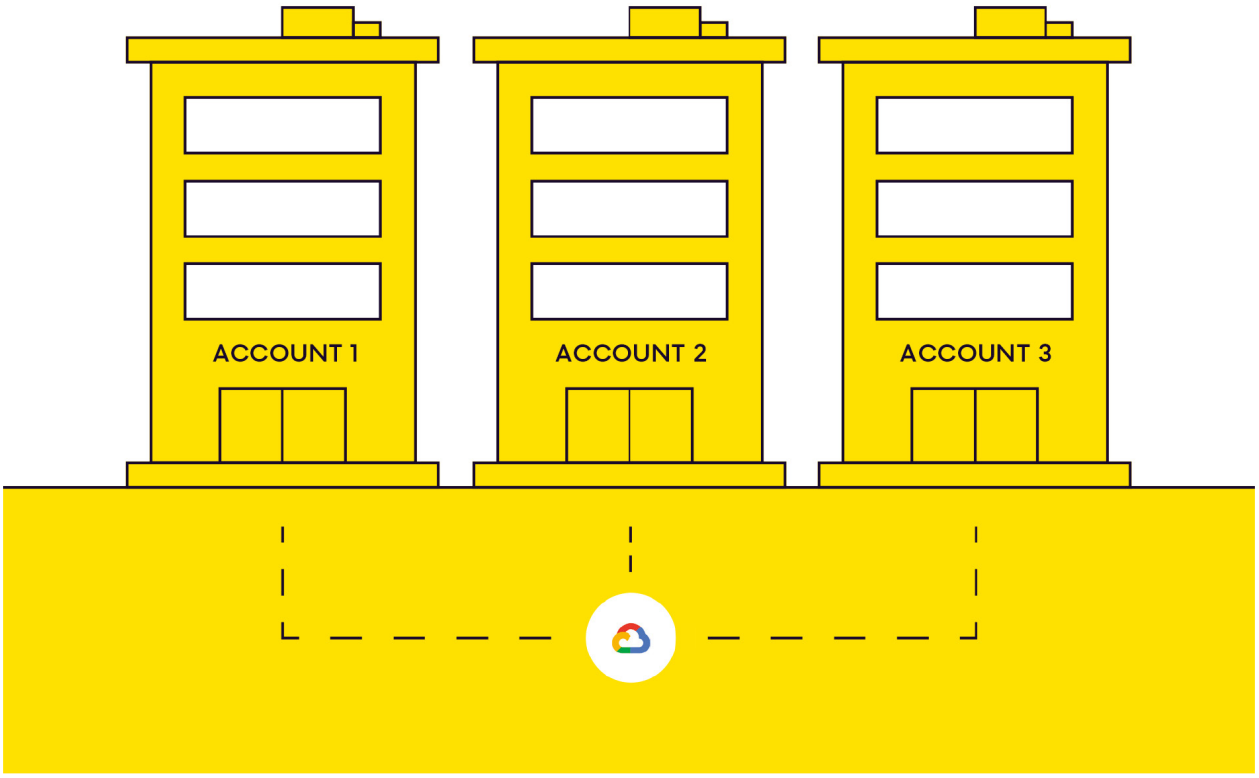
Additional security features available as add-ons:

- Single Sign-On (SAML2)
- Audit Logs: Application

Single tenant Instances

Single tenant instances are like separate buildings that only share the electricity supply. Each instance is managed within a separate capacity while being powered by GCP.

Our single tenant instances are for multinational brands that require a higher level of data security and may face tougher data scrutiny.



Within our private instance, data layers are logically separated on the back end. The computing resources reserved for the client are separated from other resources on the back end by namespace.

Single tenant instances are encrypted at the level of GCP infrastructure and undergo periodic security scans and pen tests.

To access the account on the single tenant instance, users must choose a strong password and may use two-factor authentication (2FA) to sign in. The accounts are further secured by Captcha to fend off bot attacks.

The admin of the particular project can also specify in the access management which users can see PII (personally identifiable information) of their customers. This segregation is on the front end and back end. It also supports Single Sign-On (SSO) to meet security standards in this industry.

Single tenant Instance Features

Computing Power: Reserved (Partially Dedicated/Partially Shared) Private instances include all of the features available for multitenant instances.

Additional security features available as add-ons:

- Single Sign-On (SAML2)
- Static IP (Dedicated Proxy)
- Virtual Private Network (VPN)
- Vulnerability scan report with access
- IP restriction (Cloud Armor)
- Audit log report access: IAM and Application
- Custom SSL

Multi-tenant Access and Security

On all multitenant instances, each account is encrypted all the way down to the GCP infrastructure level of GCP and undergo routine security scans and penetration tests.

Users are required to create a strong password (checked by a password guardian) and can include two-factor authentication (2FA) to sign in. Accounts are further secured by Captcha to fend off bot attacks. The admin of the particular project can also specify in the access management which users can see the PII (personally identifiable information) of their customers. This segregation is in the front end and back end.

Implementation Time

One significant difference between multitenant and single tenant instances is in the implementation time. An account on a multitenant instance can be set up and running in a matter of hours, while a single tenant instance account can take up to one or two months to complete.

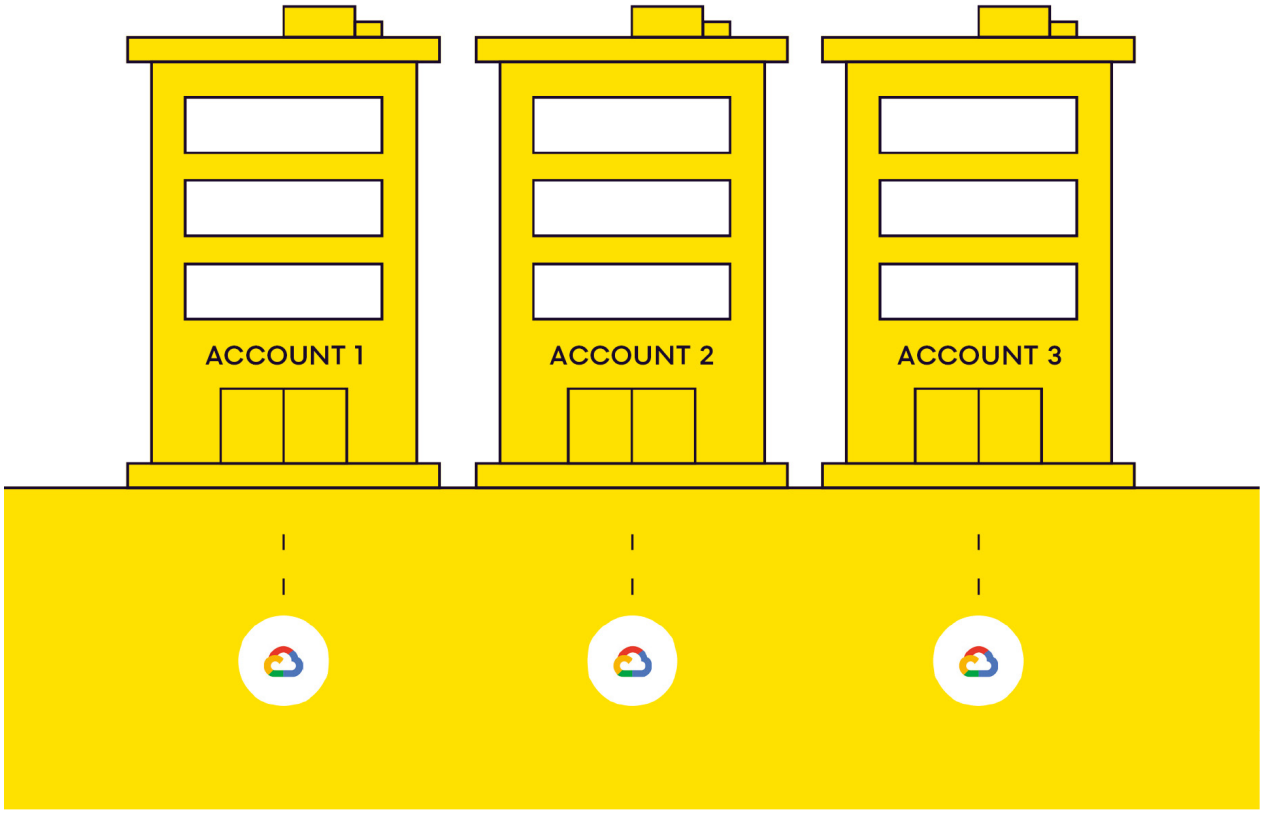
With the multitenant instance, the majority of the "ground work" is already complete and pre-configured with default security measures. Creating an account is quickly done by cloning the default account and assigning it to the individual user(s).

Single tenant instances, on the other hand, are treated as brand new environments. They are created from scratch with the unique requirements of the user(s). This requires advanced implementation services, resources, and testing to ensure that each single tenant instance is configured properly.

Exclusive Environments

Exclusive environments are like independent single office buildings with their own electricity supply. These environments are designed to manage and compute the data for a single account. With this instance type, the account is physically separated with its own hardware and managed with its own set of security protocols. Since there are no other accounts hosted on the physical server, all of the computing capacity is completely allocated to the single account.

Our exclusive environments are designed for large companies who handle sensitive categories of data and have to adhere to strict regulatory obligations.



Exclusive environments are encrypted at the level of GCP infrastructure and undergo periodic security scans and pen tests.

To access the account, exclusive instance also supports Single Sign-On (SSO) to meet security standards in this industry. The accounts are further secured by Captcha to fend off bot attacks. The admin of the particular project can also specify in the access management which users can see the personally identifiable information (PII) of their customers. This segregation is on the front end and back end.

This includes complete segregation of logical layers and network separation through utilizing a different GCP project and back-end computing resources dedicated to you. Within the exclusive instance, there is also the separation of access rights and permissions.

Exclusive Environment Features

Computing Power: Fully Dedicated

Exclusive instances include all of the features available in multitenant instances, plus:

- The client to administer their logs through hourly file exports to their SIEM
- An “emergency break” option, which gives the client the option to cut off Bloomreach Engagement from production
- Switching on new Google services / network / access rights to the back-end architecture

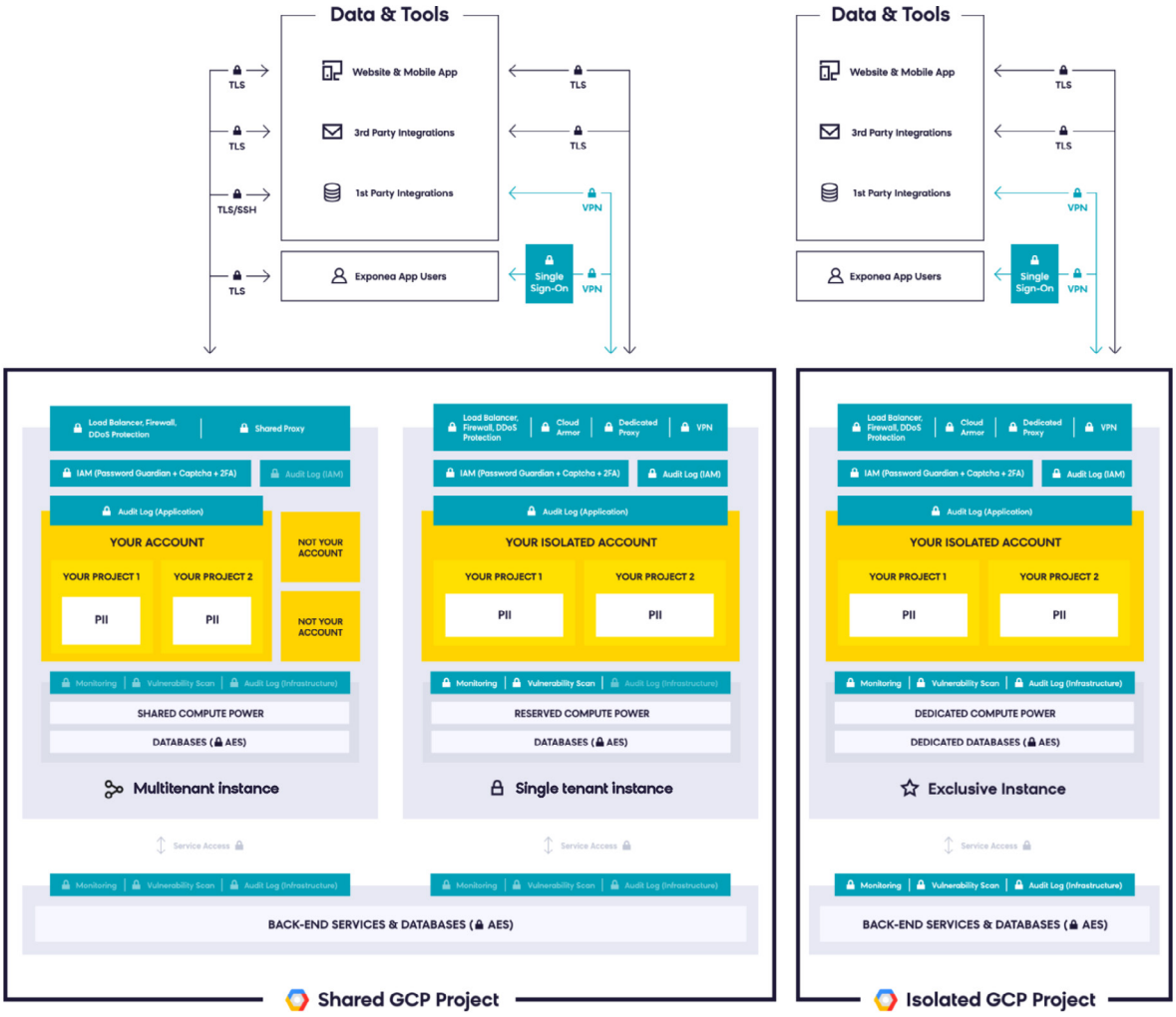
Separation Layers

The table below show the differences in the separation layers contained in each instance:

Separation Layers	Multitenant	Single tenant	Exclusive
Data Layer	Your data visible only in your accounts / projects	Your data visible only in your accounts / projects	Your data visible only in your accounts / projects
Users Layer	Users authorized only for your accounts / projects	Users authorized only for your accounts / projects	Users authorized only for your accounts / projects
Front-end Layer	Application settings, definitions, and campaigns visible only within your projects	Application settings, definitions, and campaigns visible only within your projects	Application settings, definitions, and campaigns visible only within your projects
Back-end Layer	Shared network, shared databases, shared Kubernetes cluster	Logically separated network and all back-end services, shared and dedicated databases, shared Kubernetes cluster	Network separated from scratch, dedicated databases, dedicated Kubernetes cluster
Infrastructure Administrator Access	Shared administrator accesses	Shared administrator accesses.	Administrator accesses established from scratch

Bloomreach Instance Visualization

The following visualization illustrates the differences between the three instances. The upper portion details how data in transit is secured and encrypted before entering Bloomreach Engagement, while the lower part shows a high-level overview of Bloomreach Engagement architecture and security features for each instance.



Security Features

Security Features

Bloomreach provides a comprehensive set of security features to ensure that your customer data remains safe.

Our core security features ensure endpoint security, vulnerability management, quality assurance, monitoring, and incident management.

Audit Logs and Access

The audit log offers detailed chronological records of all user information and activity within the Bloomreach application. Using the audit log provides proof of GDPR compliance and operational security. It also serves as a source of information for audit investigations and to identify the origin of any security incident.

Audit logs are operational on all instance types. However, there is a difference in the level of accessibility between the two.

Multitenant instances undergo the same audits for application, data, and communication security that occur on the single tenant instances. This process is run across accounts within the instance and managed by the Bloomreach

team, who will ensure that all security and data points are secure and archive the reports of each audit. Should an exceptional issue occur, a multi tenant user can request an account specific report for an additional fee.

Users of the single tenant instance will be able to access their logs at any time since the audit results will only ever contain the data of their specific account. However, it is the responsibility of the single tenant instance account holder to interpret the audit logs. This is typically preferred when the client has in-house IT resources that they are willing to dedicate to the task.

- **Audit Log is operational on all instances** (it runs on all systems, but access to the logs is dependent on the type of instance used)
- **Multitenant Instance -** access only to the application audit log
- **Single tenant Instance -** access to IAM and application audit log reports
- **Exclusive Instance -** access to IAM, application, and infrastructure audit log reports

For further details, go to the audit log article.

Vulnerability Scan (Tenable Nessus)

For scanning your exposure to threats, we use an enterprise vulnerability scanner from GCP. The vulnerabilities detected include coding flaws, missing security packages, malware, and insecure server configurations. Additionally, this feature provides procedures to fix the identified vulnerabilities.

- The vulnerability scan is operational on all instances
- Access to reports are available on single tenant and exclusive instances

Virtual Private Network (VPN)

Our site-to-site VPN allows you to safely connect multiple local area networks (LAN) in different locations together using a Cloud VPN tunnel.

This feature protects logins to the Bloomreach application, preventing unauthorized access to single tenant instances. Compared to a remote access VPN, the site-to-site VPN eliminates the need for each device in a network to run their own VPN client software, is easier to scale,

and the latency of the network is much lower.

The VPN tunnel can also be used as an additional security layer for data imports and API calls from campaigns.

VPN forms an integral part of our integration protection.

> Available on private and exclusive instances

Bloomreach Single Sign-On (SAML-based SSO)

For large enterprises, it is difficult to manage employee access, permissions, and resources in multiple places. Single sign-on (SSO) ensures that only authorized users will have access to the Bloomreach application. The main benefit of SSO is that it prevents the risks created by poor password management or the risks of phishing. Moreover, it provides centralized access management, which allows you to have full control of who has access to the application.

> Available as an add-on for all instances. Read more.

IP Deny List/Allow List (Cloud Armor)

To block incoming traffic based on IP addresses and ranges, we use Google Cloud Armor, an IP allow/deny list feature.

Cloud Armor allows you to restrict or allow access to HTTP(S) load balancer at the edge of the Google Cloud, preventing malicious traffic from consuming resources and entering your virtual private cloud (VPC) networks. You can also use it to control access based on IPv4 and IPv6 addresses or CIDRs and to restrict the ability of different IPs to log in to Bloomreach.

Google Cloud Armor also provides DDoS protection.

> Available as an add-on for single tenant and exclusive instances

Captcha

Blooomreach utilizes Google reCAPTCHA to differentiate between a human and a computer, therefore preventing automated and potentially malicious bots. Utilization of Captcha helps to prevent Distributed Denial of Service (DDoS) attacks by using risk analysis to differentiate humans and bots, therefore making your data more secure.

> Available on all instances

Denial of Service (DoS) Protection

Bloomreach supports protection through Google Cloud Armor, which is an enterprise-grade DDoS defense. This defense is built in against Layer 3 and Layer 4 infrastructure DDoS attacks with the Global HTTP(S) Load Balancer.

> Available on all instances

Firewall

Most GCP servers are only available on the internal network. Services and servers with external IP addresses are automatically scanned and analyzed on a regular basis. Services that should not be available to the public are blocked by GCP Firewall.

> Available on all instances

Integration Protection

Bloomreach Integration Protection offers multiple security features to ensure the privacy and security of your data when transferred over the internet and imported into the application. This ensures that your data is always safe and protected from various forms of potential cybersecurity threats.

Static IPs (Proxy)

Bloomreach platform runs in the cloud with a wide range of external IP addresses. If you are regularly importing data (URL, database, etc.) from your own servers into Bloomreach, or firing webhooks from Bloomreach to your servers, a proxy server with static IP allows you to whitelist specific Bloomreach server IP addresses to make sure that no one else on the internet can access your data on your servers.

Webhooks and URL imports are fully supported. For database connections in support of static IPs, refer here.

> Available on all instances

TLS/HTTPs API

The Bloomreach application utilizes TLS security protocol for communication within the app and web tracking. TLS is a security protocol designed to facilitate privacy and data security for communications over the internet.

HTTPS uses TLS (SSL) to encrypt normal HTTP requests and responses, making data movement safer and more secure. Data is encrypted in transit in both directions: going to and coming from the origin server. It is beneficial to use HTTPS as it is more trustworthy for users, since it guarantees that a website server name is authentic. As a result:

- Attackers cannot steal or phish data
- The user's usernames and passwords can't be stolen in transit when us ers enter them into a form
- Available on all instances

SSL Certificate

SSL certificate verifies that a client is talking to the correct server that actually owns the domain for tracking and logging into the Bloomreach application. An SSL certificate is a data file hosted on a website's origin server, containing the website's public key and identity.

This feature is beneficial for your security as devices attempting to communicate with the origin server can verify the server's identity. On single tenant instances, SSL is also available with your own SAN certificate.

Bloomreach uses the certification authority Let's Encrypt to issue certificates as a default option. We also provide an option to use a custom certificate authority.

- Available on all instances

SSH

SSH tunnel provides protection for the data you transmit via the internet and import into the Bloomreach application. It is much more secure to use a SSH tunnel as the only gateway to your network rather than leaving your databases and ports open to the internet.

- Available on all instances

Security Comparison Table

		Multitenant	Single tenant	Exclusive
Infrastructure	SIEM	✓	✓	✓
Security	Regular penetration testing by 3rd-party companies	✓	✓	✓
Data Storage	Encryption at rest	✓	✓	✓
	Backups	✓	✓	✓
Data Access	Audit log		✓	✓
	IP allow/deny list (Cloud Armor)		✓	✓
	Bot protection (CAPTCHA)	✓	✓	✓
	Unusual activity monitoring (SIEM)	✓	✓	✓
Portal Access	TLS	✓	✓	✓
	Single sign-on	✓	✓	✓
IAM	MFA + role enforcement	✓	✓	✓
	Granular roles	✓	✓	✓
	Access management	✓	✓	✓
	Password policies	✓	✓	✓
	VPN		✓	✓
Data flows protection	SSH	✓	✓	✓
	Static IPs (socks proxies)	✓	✓	✓
	HTTPS for APIs	✓	✓	✓

The default option is a multitenant instance. Other instances are available for an additional cost.

Audit Log and Vulnerability Scan is operational on all instances (it runs everywhere, but access to it may not be available on some instances).

Consistent Security Across All Instances

It may seem multitenant instances have larger attack surface, but it's not the case. The main difference between the two instances is in the level of access to the routine vulnerability scans and audit logs that operate in the back end.

With multitenant instances, your account will undergo the same protocols for application, data, and communication security that occur on exclusive environments. Bloomreach will store the reports and security logs on our end. Access to the audit reports can be delivered upon request under a non-disclosure agreement (NDA).

Should an issue occur, our Bloomreach Security team will promptly notify you of the situation and take remedial action to restore the integrity of your instance.

Bloomreach Engagement Enterprise Security

Bloomreach Engagement Enterprise Security

We understand some of our clients require additional security. When working with sensitive data, such as banking or telecommunications sector data, we implement extra measures to increase the level of security of their data.

We provide an additional layer of features for enterprise clients, including enhanced security and access management.

Both our core and enterprise security utilize our private and public APIs, which enable you to control your customer's data.

Using our dedicated Bloomreach Engagement private API, you can securely send and download data from Bloomreach Engagement, allowing you to fulfill Subject Access Requests required under GDPR.

We use both a public and private API:

- Our public API is used for web tracking and web personalization, and uses a public token
- Our private API uses a private token and API secret

Security Management

Security Management

We take care that all of our endpoint devices are protected according to our Endpoint Security Policy. This includes that all of our endpoint devices have disc encryption, malware protection, guest access disabled, firewall, and have regularly updated OS. In addition, we perform regular checks to make sure that we maintain this high level of security.

Monitoring

Our security monitoring is performed on information collected from internal network traffic and the knowledge of our vulnerabilities. Internal traffic is checked for any suspicious behavior. Network analysis and examination of system logs in order to identify unusual behavior are a vital part of monitoring. We place search alerts on public data repositories to look for security incidents and analyze system logs.

Vulnerability Management

Bloomreach Engagement has a vulnerability management policy that includes processes such as regular web scans and scans for potential threats. Once a vulnerability requiring our attention has been identified, it is tracked, given a priority according to how urgent it is, and assigned to relevant people as a ticket. Our security team tracks such issues and follows up regularly until they can check that the issues have been resolved.

Incident Management

Bloomreach Engagement has well-defined incident management processes for security events that may affect the confidentiality, integrity,

or availability of our clients' resources or data. If an incident occurs, the security team identifies it, reports it, assigns it to the correct resolver, and gives it a resolution priority based on its urgency. Events that directly impact our customers are always assigned the highest priority and shortest resolution time. This process involves plans of action, procedures for identification, escalation, mitigation, and reporting.

Security Culture

Security Culture

We have always taken the topics of security and privacy at Bloomreach Engagement very seriously. It is our highest priority to protect the data we work with, including our clients' data. We strive to always use the highest measures so that we stay secure and compliant. Security shapes our structure, educational objectives, and the recruiting process.

Security as Our Priority

We are trying to create a strong security culture among all employees of Bloomreach. We strongly believe that every employee is an essential part of our defense against potential security breaches.

This culture has a strong impact on all employees and is present at all stages and everywhere, including the hiring process, employee onboarding, and the ongoing training that Bloomreach provides, as well as company events to raise awareness. Before an employee joins Bloomreach, we perform a check of their background. All our employees must be familiar with our security policies and go through security training as part of the onboarding process, and also receive regular security training throughout their stay here at Bloomreach. During the onboarding process, new employees agree to our NDA and go through OWASP training. This shows our commitment to keeping the data of our customers secure.

All employees working at Bloomreach must follow our password security and lockout policy, must have 2FA authentication, and must have a secure Wi-Fi connection (or alternatively, be connected to our VPN when working remotely). Additionally, all of Bloomreach's employees are using Okta, which is an SSO service that enables them to securely access their accounts and applications.

Security Development Practices

The developers in the IT segment receive instructions on topics like best coding and development practices, the principle of least privilege when granting access rights, etc. The IT department also attends technical presentations on security-related topics, and receives regular updates on the newest issues from the cybersecurity space in our Security channel.

SOC 2 Report

Bloomreach Engagement holds a SOC 2 report which goes into depth about technical security measures in our application's infrastructure and organizational security measures in the company. You can access the report with an NDA in place.

Security Operations Team and the DPO

Bloomreach Engagement has a dedicated team that consists of Security Engineers and a Security Manager who is an essential part of our IT. This team is responsible for maintaining Bloomreach Engagement's protection and defense systems, reviewing security operational processes, building security frameworks, and creating new security policies. They also monitor any suspicious activity, address cybersecurity threats, and perform regular health checks and audits. Our independent Data Protection Officer (DPO) makes sure that Bloomreach Engagement stays compliant. The DPO is tasked with monitoring compliance with the GDPR and other data protection laws, our data protection policies, GDPR awareness training, and audits.

Conclusion

Conclusion

The information and procedures provided in this whitepaper describes the commitment that Bloomreach has towards the protection and confidentiality of your data. Our internal security teams, along with the native security protocols implemented within Google Cloud Platform, are dedicated to safeguard your data so you can focus your time and resources towards managing your business. With Bloomreach, you can be assured that you have a partner who will help you serve more customers, achieve business outcomes, and scale quickly, all while having the peace of mind that your data is safe and secure.

Explore more of our security commitment.


bloomreach