ZAP REPORTS

Zap Reports Security

Overview

Zap Reports is a multi-tenant Software as a Service designed to get companies the documents they need. As this service deals with sensitive information, security is placed at the forefront of the Zap Reports platform and is taken into account at every level of the development and operational processes. This document outlines the protocols that govern how Zap Reports operates and manages its services.

Infrastructure

Zap Reports is a cloud- based platform built to scale as the demand for its offering changes. As such, the service can be accessed via domains controlled by Zap Reports as well as remotely via its open API connection. Due to the nature of these web services, a grouping of servers is publicly accessible to the Internet and allows for inbound and outbound traffic. To mitigate the risk of malicious behavior by outside parties, all servers are outfitted with tested and reliable code at the application level to reject unauthorized access to server data. Zap Reports demands high internal standards for code quality, mandatory code reviews, and constant internal security consultations on complex technical decisions. Servers are monitored by a third-party service to alert the administrator based on any unusual activity. Zap Reports reviews and updates its code and systems configuration to ensure your data is always protected. Zap Reports works with a leading cybersecurity firm that tests our platform using the most advanced techniques available to ensure that its software is secure.

Further, Zap Reports maintains continuous back ups on all of its datasets, and has also established multiple, geo-redundant sets of database replicas to be automatically deployed should a primary database attack or failure occur. Through penetration/vulnerability testing and monitoring and data redundancy, Zap Reports is able to ensure data security.

Network Access

All Zap Reports servers reside inside a virtual private cloud and use a NAT gateway to route all payloads through a single unified IP address. All databases used by Zap Reports immediately reject any connection attempts coming from an address outside its list of allowable IP’s to further secure against any outside attack or unauthorized attempt to collect data. Zap Reports hosting facilities are audited annually for security certifications (such as SOC 2 and ISO27001) to ensure they employ advanced physical security measures such as biometrics, CCTV cameras, and 24×7 on-site security.

Data Separation

Zap Reports has invested heavily in a proprietary application-based logic model with the sole purpose of keeping data separate among tenants inside the software. Put another way, this means that while many different tenants may use Zap Reports, Tenant A will never be able to view the data of Tenant B. Inside the dashboard, whenever a request is made to retrieve data, the requestor is first validated as an authenticated and logged in user. If this validation succeeds, a request to return data will only bring back data that is marked with the user’s unique tenant ID. Checks have been put in place to confirm this match and endpoints are developed in a way to clear data before it returns if this check is not found to be successful.

Brute Force Attacks

All requests to Zap Report servers undergo strict rate limiting and CORS validation. This is to not only ensure a high level of service for all customers of Zap Reports, but to automatically limit and reject the likelihood of brute force attacks succeeding. Authentication to the dashboard is only allowed from Zap Reports controlled domains and only 10 unsuccessful requests to log in may be made every 15 minutes. Zap reports will automatically lock a user's account for a period of time after too many failed login attempts.

Secure Socket Layer

All servers and websites in use by Zap Reports employ a Secure Socket Layer (SSL) encrypting the data that is exchanged between clients and servers inside the Zap Reports Ecosystem. Zap Reports applies in-transit and at-rest encryption using industry best practices (such as HTTPS and TLS) to ensure your firm's data is stored and transmitted securely. Our web interfaces are also verified by Let's Encrypt, a trusted certificate authority.

User Permissions

All tenant companies within Zap Reports have the ability to limit users within their organization from being able to access sensitive information within their organization's account. This allows for a business owner or manager to adjust how modifications can be made to their dashboard.

Passwords and Connecting Keys - Zap Reports

All passwords and connection keys (API Secret Keys) are stored via a one-way hash that cannot be reversed. No employee or admin of Zap Reports can ever read the actual value of a password. Should a data breach occur, the party who obtained the data should not be able to reverse the hash and will therefore have no useful information related to any user's password or connection keys.

Zap Reports encourages frequent password changing and rolling of API keys as a best practice. In the event a user believes a password or connection key has been compromised, the user can easily reset the password by clicking on the forgot password link or logging in to the dashboard and accessing the security settings.

Passwords and Credentials - Financial Institutions

During the course of an end user's journey through Zap Reports the user may have the option to log into the user's financial institutions and payroll providers, collectively referred to herein as "Data Sources", to allow Zap Reports to access data. Zap Reports realizes the need to keep this information safe and has put in place different protocols that ensure the highest level of security is given to protecting an end user's credentials.

Below is an explanation of the types of connections with Data Sources as well as processes put in place by those Data Sources.

Connection Types: Credential / Open Banking

Zap Reports connects to thousands of financial institutions all offering their own protocols, means of connection, and security. Two primary methods are used by Zap Reports to maintain connections with financial institutions.

Credential Based connections work just the way they sound. By utilizing a user's login credentials, Zap Reports can access the user's accounts to return pull data. In some instances, this approach also involves a form of multi-factor authentication (MFA) to succeed and by which the user will need to be present and provide a texted/emailed security code or answer any number of security questions.

Open Banking / OAuth connections differ from Credential Based authentication in that Open Banking utilizes a tokenization process to provide access to account data. After a user logs into a financial institution for the first time using an OAuth Based connection, the security information is stored in a token that encrypts the user’s actual credentials so that the credentials cannot be accessed. Zap Reports and our partners actively work to utilize this connection whenever possible as it provides the most reliable security protection.

Zap Reports believes in full transparency to our users about their data and the security around it. If at any time a user does not want to keep a connection open to an online banking account, the user can use their Zap Reports portal to remove any or all connections previously established.

Bank Security

The vast majority of banking institutions today require both credentials PLUS another authentication method to allow the transfer of money or to make a change to an account. Banks routinely require presentation of a form of ID such as a driver's license or require an action such as a confirmation via an emailed/texted security token to permit any action beyond accessing the account.

Zap Reports Staff and Physical Premises

Zap Reports enforces a set of administrative, physical, and technical controls such as office access policies, two-factor authentication for internal tools, criminal background checks for employees, regular security training, and more. Staff members within Zap Reports are given access only to the information they need to perform their role within the company. Only the highest level of developers can access information regarding servers, databases, and infrastructure within the Zap Reports Ecosystem.

Ongoing Security Efforts

While Zap Reports has invested heavily into security, it does not mean we are done improving. Continued efforts such as 3rd party audits, code testing, and use of outside compliance counsel have been and will remain top priorities as Zap Reports grows.

Any security related concerns or questions can be directed to CTO and co-founder, John Maher, at john@zapreports.com.

Disclaimer

Although Zap Reports has attempted to provide accurate information and guidance in this document, we provide no warranty related to its content. The implementations, procedures, and policies of Zap Reports are subject to change and may impact the information reflected in this document. The rights and responsibilities of the parties with regard to your use of the services shall be set forth solely in the applicable Zap Reports Terms and Conditions as they are posted from time to time at ZapReports.com. Customers should make their purchase decisions based upon features that are currently available.