siftery Track

Information Security and Data Privacy

April 2018

Siftery Inc.
855 Folsom St, Suite 108
San Francisco, CA 94107

Infrastructure & Security

Data Encryption and Hashing

Track uses bank-level security to ensure your data is safe. This includes 256-bit encryption for data in transit for all the APIs and export options we support. For direct connections to financial institutions, we use the Plaid API that only allows client requests using strong TLS protocols and ciphers. Additionally, all communication between Plaid infrastructure and financial institutions is transmitted over encrypted tunnels and all client communication with Plaid's API utilizes cryptographically hashed headers and timestamps to verify authenticity. We also never store passwords and other auth creds as clear text - they are always hashed and salted securely.

Active Monitoring and Threat Mitigation

Track uses industry-best logging, intrusion detection and mitigation platforms for both infrastructure and application level events. For infrastructure-level events, we employ McAfee for endpoint threat monitoring, defense and response. For product-level events, we employ Sqreen for in-app intrusion detection to block attacks in real-time and automatically isolate user accounts at risk. Additionally, we use SumoLogic for centralized logging and continuous monitoring across the entire stack to detect and contain indicators of compromise (IOCs) such as account takeover attacks, password bruteforce, or stolen credentials in real-time. We can also provide end-user auditable logs of key activities within a workspace upon request.

Cloud Security

Track is hosted on AWS and inherits the physical security of the largest cloud services operator. In addition to enforcing strict employee data handling policies, we natively limit administrator access for our production environment to just the CTO and two lead architects. Separate access controls are also applied at each layer of infrastructure via detailed IAM policies. All application and user access logs are stored centrally and monitored, and are made fully available for external security and privacy audits. Additionally, we employ CloudSpolit for automated AWS security and configuration monitoring, and conduct regular vulnerability and penetration testing by reputed third parties.

Infrastructure as Code

To respond faster to unavoidable server and security issues, Siftery applies the practice of infrastructure-as-code where all of our configurations or recipes are stored and edited through code. Provisioning of infrastructure and deployment is fully automated via an industry-leading stack that includes Chef, Terraform and Semaphore.

Network and Device Security

Access to Siftery's production, staging and sandbox environments is controlled through a VPN and we require all engineers to use multi-factor authentication (MFA) for the VPN and their personal devices. We also mandate full-disk encryption for all employee laptops and development devices.

Privacy & Account Controls

Information Privacy

As a policy, Siftery Track doesn't require any Personally Identifiable Information (PII) beyond that required to set up an account (name and email). Any and all data that flows into your dashboard via API syncs or manual uploads is treated as private, and is never shared with anyone else without your explicit permission. You retain ownership of all the data that flows into your dashboard and can choose to delete all or parts of it at any time. If you use our concierge onboarding, an additional NDA is executed to restate our commitment to your privacy and ownership.

Data Handling

As a company that handles data of sensitive and confidential nature, Siftery is keenly aware of its custodial obligations. We have built a development process that requires minimal manual intervention, is constantly monitored, allows rapid response to issues, and encourages efficient software testing. We extensively utilize multiple staging and sandbox environments with mock data, with production data both isolated (never gets into staging or testing flows) and containerized (for each customer).

While we make sure every one of our employees understands their personal role in keeping your data safe from security compromises and data breaches, we additionally require every employee with even partial privileges to our production environment to sign NDAs and confidentiality agreements that are reconfirmed annually. Please email us at privacy@siftery.com for a copy of the NDA and confidentiality agreement.

API Access

Siftery Track is a read-only app that is not designed to make changes, trigger activity or write data back to any of the accounts you sync. For all the APIs we provide sync support for, we request limited access to your accounts only to the extent of analyzing your expense transactions and utilization data where applicable. This means that no one, including you, can use the service to access money or make changes to any of the accounts.

Account Controls

Siftery Track provides you full control of your data, including the ability to delete a particular account you synced, the entire workspace you created, or all of your workspaces and user accounts associated with them. For every workspace you create, you have full control over who else has read and write access to it. The application interface makes it easy for you to share your dashboard and insights with others in your team, but also allows you to modify access permissions as you choose at any time.

McAfee SECURE

sumologic

Protected by sqreen