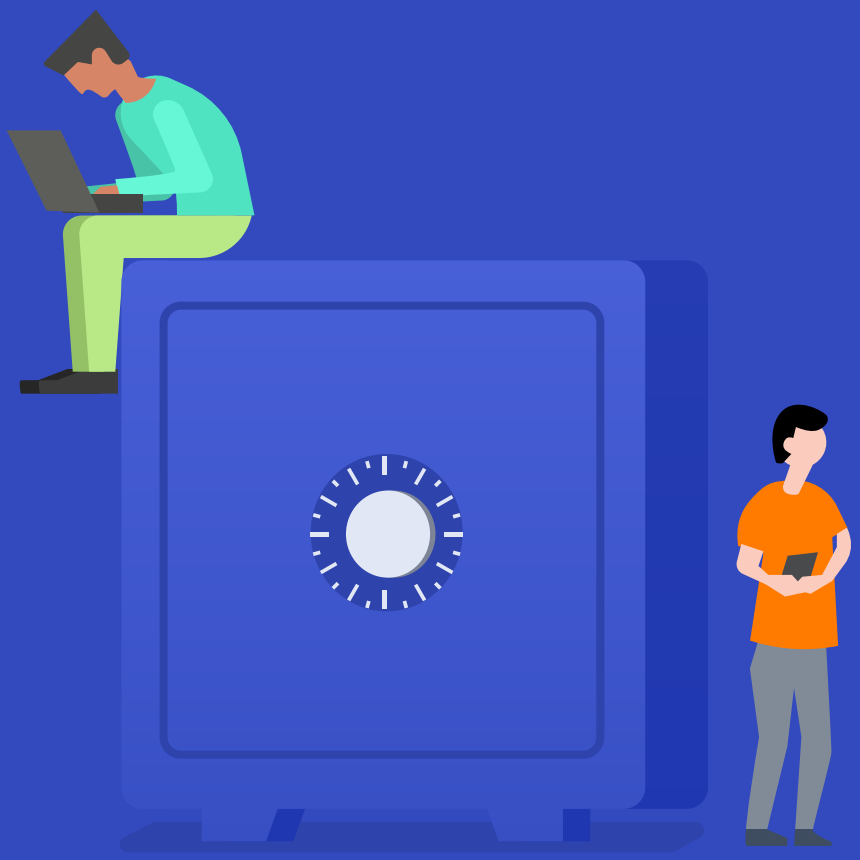
siftery Track

Information Security and Data Privacy



Introduction

At Siftery, we take the responsibility of securing customer data very seriously. In our pursuit to build a security first infrastructure as well as a security-focused operational culture, we are currently implementing security measures that will meet and exceed the security objectives required for SOC2 certification. The document lists down progress we have made in the last 6 months.

Information Security Program

Data Centers

Infrastructure

Siftery is entirely hosted on Amazon Web Services (AWS) and inherits the physical security of the largest cloud services operator.

Redundancy

AWS data centers are designed to anticipate and tolerate failure while maintaining service levels. In case of failure, automated processes move traffic away from the affected area. Core applications are deployed to an N+1 standard, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

Server Operating System

Siftery uses a Linux (Ubuntu) based operating system for the application environment with a centrally managed configuration orchestrated via Hashicorp's Terraform. Siftery has established a policy to keep systems up to date with necessary security updates.

Business Community

Siftery's Business Continuity Plan builds on top of AWS's own Continuity Plan, and outlines measures to avoid and lessen environmental disruptions. It includes operational details about steps to take before, during, and after an event. During and after testing, Siftery documents people and process performance, corrective actions, and lessons learned with the aim of continuous improvement.

Network and Transmission

Siftery uses industry standard encryption schemes and protocols to encrypt data transmissions between different servers. This is intended to prevent reading, copying or modification of the data.

Intrusion Detection

Siftery employs Intrusion detection system to provide insight into ongoing attack activities and to help remediate the attack faster. We use Threat Stack (threatstack.com) to achieve:

- Real-time cloud configuration auditing
- Host-based intrusion detections
- File integrity monitoring
- Vulnerability assessment
- Threat intelligence correlation

We are able to detect suspicious activity, like misused AWS keys or servers spun up in unused regions, to give us the ability to track the attacker as they jump back and forth from the host.

Incident Response

Siftery's security personnel (led by our CTO) will promptly react to discovered security incidents and inform the involved parties.

Encryption Technologies

Siftery's servers support HTTPS encryption and TLS1.2. Further to this, data is encrypted at REST and encrypted in transit. AES is used to encrypt the user tokens at the database level.

Site Controls

Data Center Security Operations

All data centers in use by Siftery maintain 24/7 on-site security operations responsible for all the aspects of physical data center security through AWS. All AWS data centers comply with or exceed the security requirements of SOC2 and SOC3. All AWS data centers are equipped with CCTV, on-site security personnel and key card access system.

Access Control and Privilege

Siftery's administrators must authenticate themselves via a central authentication system or via a single sign on system in order to administer the Services.

Internal Data Access Processes and Policies

Siftery's internal data access policies are designed to prevent unauthorized users or systems from getting access to personal data. These policies are in the process of being audited by an independent auditor.

Siftery follows the principle of least privilege and active segregation of duties between Developer Operations (infra) and Development (code). 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.

Siftery employs a centralized access management system to control access to production systems and server, and only provides access to a limited number of authorized personnel. SSO and SSH certificates are used to provide secure access mechanisms. Siftery requires the use of unique IDs, strong passwords and two-factor authentication. Granting of access is guided by an internal policy. Access to system is logged to provide an audit trail for accountability.

Change Control Procedures

All changes to the Siftery Track application and related infrastructure goes through a formal change control process in order to minimize the risk associated with such change.

- Continuous source-code integration and asynchronous deployment post a documented team-lead review of code
- Automated testing, recording and alerting of results
- Lock-out from customer data
- Comprehensive logging and near real-time review of alerts

Vulnerability Testing

Siftery undergoes an independent vulnerability audit and penetration testing twice per year conducted by 3rd party security research companies (Umercs).

In February 2018, the Siftery Track application underwent a comprehensive and independent baseline security assessment. The overall goal was to enumerate and categorize all weaknesses within the application that could be leveraged by an attacker to compromise, or otherwise impact the availability of the Track application.

The assessment was conducted over a five-phase project. At the core of the assessment...	• The external footprint of the company was analyzed • An active vulnerability assessment exercise took place over the course of a week • A comprehensive review of the AWS configuration was done and remediation steps published • A simulated phishing attack was conducted over key engineers, product managers and executives

Based on the findings, a remediation plan was put into motion to address the most significant findings. At the end of the assessment, it was noted that the externally facing Track application did not exhibit any critical findings that would put any customer or data at imminent risk.

Responsible Disclosure

The disclosure of security vulnerabilities by independent researchers helps us ensure the security and privacy of our customers.

Siftery requires that all researchers:

- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction of data during security testing
- Perform research only within the called out scope in the disclosure policy
- Use the identified communication channels to report vulnerability information to us, in our case it is security@siftery.com
- Keep information about any vulnerability a researcher has discovered confidential between the researcher and Siftery until we've had 30 days to resolve the issue

Reporting a Security Vulnerability

If a researcher believes they've found a security vulnerability in one of our products or platforms, we request them to send us the vulnerability by emailing security@siftery.com.

We request the following to be included at the very least as details with a security report:

- Description of the location and potential impact of the vulnerability
- A detailed description of the steps required to reproduce the vulnerability (POC scripts, screenshots, and compressed screen captures are all helpful to us)

In the interest of the safety of Siftery's users and employees, the following test types are excluded from scope:

- Findings from physical testing such as office access (e.g. open doors, tailgating)
- Findings derived primarily from social engineering (e.g. phishing, vishing)
- Network level Denial of Service (DoS/DDoS) vulnerabilities

Data

Data Storage and Isolation

Siftery stores data in logical multi-tenant database environments on AWS. The data is replicated on multiple redundant systems too, especially with periodic automated backups.

Data Handling and Privacy

As a company that handles data of sensitive and confidential nature, Siftery is keenly aware of its custodial obligations. Principle of least privilege is always at play. Siftery utilizes multiple staging and sandbox environments with mock data. Real customer data is isolated and logically partitioned for each customer.

Siftery HR policies ensure every one of its employees understands their personal role in keeping customer data safe from security compromises and data breaches, Siftery additionally require every employee with even partial privileges to our production environment to sign NDAs and confidentiality agreements that are reconfirmed annually.

Data Ownership

SifteryTrack provides a customer full control of their data, including the ability to delete a particular account that a customer has connected, the entire workspace(s) created by them, or all of the their workspaces and user accounts associated with them, at any point of time.

For every workspace a customer creates, they have full control over who else has read and write access to it. The application interface not only makes it easy and elegant for the customer to share a dashboard and insights with others in their team, but also allows them to modify access permissions as the customer chooses at any time.

Data Sources

For direct connections to financial institutions, Siftery uses financial aggregators (like Plaid and Yodlee) and ERP APIs like Intacct, Quickboos, Expensify etc. All communication between Siftery's infrastructure and financial APIs are transmitted over encrypted tunnels and utilizes cryptographically hashed headers and timestamps to verify authenticity.

Personnel Security

Siftery personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Siftery's confidentiality, privacy and acceptable use policies. All personnel are provided with security training upon employment and then regularly afterwards. Siftery's personnel will not process customer data without authorization.

Application Security

User Authentication and Passwords

All user passwords are encrypted and salted. Siftery authenticates all users with a unique ID and password.

RBAC (Role Based Access Control)

User Scopes: Several scopes exists to restrict the GraphQL API access for these levels – normal user-scope, admin-user scope, organization scope, and are set in a persistent database.

Unique Session: Each user is identified with a unique session, stored in a secure, HTTPS only, session cookie.

Session Expiry: A user session auto-expires in 30 minutes for additional security.

Attack Prevention

Siftery is able to surface in real-time various attack vectors like Cross-Site Scripting (XSS), NoSQL injections, SQL injections, data exfiltration, account takeovers, brute force attacks, through a combination of AWS firewalls, and Sqreen.io.

Epilogue

The Security practice at Siftery is a continuous endeavor to keep up with the changing landscape of information security. We continue to bring in more leadership and adopt better tools, techniques, and standards spanning our policies, operations and people.

For feedback and questions, please reach out to security@siftery.com or ayan@siftery.com directly.