sift

Security Framework

Security and privacy are fundamental to our product development and business operations. Our customers entrust us with keeping their data safe, and protecting this data is a top priority for Sift. This document provides you with information about our general security practices, the security of your data, and how you can obtain more information.

Certifications:

Core Principles

While all our employees have an obligation towards security, our Engineering, Legal and Compliance teams are responsible for securing customer data. Together, these teams have built Sift's security framework on three core principles: confidentiality, availability, and integrity.

Confidentiality — we protect your data.

We have implemented the following controls in order to protect customer data:

STATE-OF-THE-ART INFRASTRUCTURE

Sift's technology, data, and infrastructure are hosted on data centers maintained by Amazon Web Services (AWS) and Google Cloud Platform (GCP). These data centers offer state-of-the-art physical protection for the services and related infrastructure that comprise the operating environment for our services. You can learn about AWS's security and controls by visiting the AWS Cloud Compliance website and GCP's security and controls by visiting Google Cloud Trust and Security

PHYSICAL SECURITY

All physical servers are located on the AWS platform. AWS offers 24x7 surveillance, security logs, and multi-factor authentication. Sift's office resides in a building with 24x7 security.

DATA ENCRYPTION

We support the SSL/TLS protocol to encrypt user data in transit. We also encrypt all data at rest. We use OAuth 2 for authentication of the Sift application, and authentication data is encrypted using bcrypt.

RESTRICTED ACCESS

Our production systems and database infrastructure are accessible only to those Engineers who require access to improve our product and service. Our application environment and internal tools are protected by a Virtual Private Cloud (VPC). Users must authenticate with the VPN using unique user credentials and multi-factor authentication.

CUSTOMER DATA SEGREGATION

We keep each customer's raw data logically separate from that of other customers. Our systems were built to ensure that customers may never view other customers' private data. Sift shares only learnings and other derived data between customers in order to more effectively fight fraud.

INFORMATION SECURITY POLICY

We maintain a comprehensive, organization-wide set of information security policies and procedures. Policies include access control, change management, network security, incident response, and hiring.

Availability — we operate a redundant application architecture.

Sift strives to provide a resilient and highly available service to our customers across the globe who rely on us each and every day to prevent online fraud. Attributes of our service that contribute to our high availability include:

ARCHITECTURE

We've designed our systems for scalability. Our API servers have very few dependencies and operate on a queue-based architecture to ensure that we can ingest customer data even during times of network or system instability.

24X7 MONITORING

We monitor our systems 24x7 with third-party tools. Engineers are always on call and are required to respond to notifications within 5 minutes.

BACKUPS

To prevent data loss, we replicate data across multiple locations and back up data daily to highly durable storage.

INCIDENT RESPONSE, BUSINESS CONTINUITY

We maintain an Incident Response Procedure which outlines the process, roles, and responsibilities in the event of an incident.

Integrity — we maintain the quality of the data you send us.

In order to provide customers with the most accurate fraud prevention service, Sift must ensure data quality. We use the following controls to maintain the quality and integrity of our customers' data:

CHANGE MANAGEMENT

Sift performs code reviews prior to deploying significant code changes to production. Changes that may impact system availability or security are further reviewed by the technical risk review team.

TESTING

Modifications to Sift's technology, including code and configuration changes, are tested in a staging environment prior to being implemented in our production environment.

INTEGRATION MONITORING

Sift solutions engineers monitor customer integrations to ensure that data they send Sift is well-formatted.

LOGGING

Sift logs employee access to customer data. Customers may request logs by emailing support@sift.com.

Customers may subscribe to notifications or visit our publicly available Status page to learn about planned and unplanned service interruptions as well as review service availability and latency statistics.

 |