HARNESS

SECURITY

As an enterprise-class technology platform, the security of our clients' customer data is one of Harness's primary objectives. As such, our architecture was built with security at its core. This document provides a high-level overview of the security protocols implemented throughout the data journey from the client app to the Harness Platform.

Security begins with data collection via the Harness Platform

The Harness Platform automatically collects anonymous lifecycle data: app version, device data (e.g. OS, OS Version, Carrier), and session information (session start/session end).

All data is encrypted via Transport Layer Security (TLS) for transport to the Harness data store. TLS v1, TLS v1.1 and TLS v1.2 are supported.

The Platform further ensures security by ensuring that encryption is signed by a specific Certification Authority (CA), which ensures third parties are unable to inspect data packets via proxies.

All server-to-server endpoints require encryption and authentication.

HARNESS

Access to Harness systems are controlled and secured

The ability to access Internal systems are restricted to secured users.

Only trusted, background checked operations personnel can access customer accounts, with all access logged and available for auditing purposes.

Multi Factor Authentication (MFA) via mobile tokens is required for all Harness personnel.

No non-employees have access to Internal Harness systems. No customer data is ever transmitted to employee computers.

Outbound data is sent securely

All data is sent with the strongest data encryption made available by the partner.

Whenever supported, hashed device and user identifiers are sent instead of raw identities.

Strategic Partnerships

Harness's works hand in hand with world class financial technology partners to create our technology and ensure its security. To authenticate our Round-Up Technology, Harness has partnered with Plaid Technologies, Inc. to facilitate instant account verification. To collect donations, Harness has partnered with Stripe, Inc to create a transparent and intuitive user experience.

For more information on how our trusted third parties utilize state of the art security measures to ensure our partners security, please check out their security documentation.

https://stripe.com/docs/security/stripe

https://plaid.com/security/

HARNESS

Where is data stored?

Data is spread across **Harness**, **Plaid**, and **Stripe**. All sensitive payment information (credit card or bank account numbers) is stored on **Stripe**. All other sensitive bank account information (transaction records as well as account/routing numbers) is stored on **Plaid.** Users' Harness Account login, plaid/stripe access tokens, and roundup preferences are recorded on **Harness.** User's Harness Account passwords are encrypted with the industry standard **blowfish** algorithm to prevent anyone except from the end user from knowing their password, including **Harness**.

Does my organization need to create an account?

The merchant account will be created and hosted on **Stripe**, and our partners will have complete and independent control over this account. Upon signup, they will permit **Harness** to transfer funds to their account on their behalf. **Harness** will not be able to withdraw funds from our partners **Stripe** account.

Do all third parties that Harness utilizes have secure practices?

The **Harness** API is organization agnostic; all the security applies equally to all connected organizations. Each organization is just another record in the database with their **Stripe** merchant account id attached to it, so there aren't any special case-by-case security needs. All communication to and from the **Harness** API is secured over 256-bit SSL certificates from **RapidSSL** and verified by **GeoTrust**.