wisely.
Accelerate fundraising with AI.

Data Sheet

Wisely Cloud and Data Security

Overview

Wisely is developed and built specifically for non-profits and their fundraising teams. We only leverage fully-managed cloud systems from world-class providers with dedicated security and infrastructure teams. Our focus over time will be to consistently raise the bar of our privacy and security programs to best protect your data. This document details the security protocols we've implemented for organizations using Blackbaud's Raiser's Edge NXT.

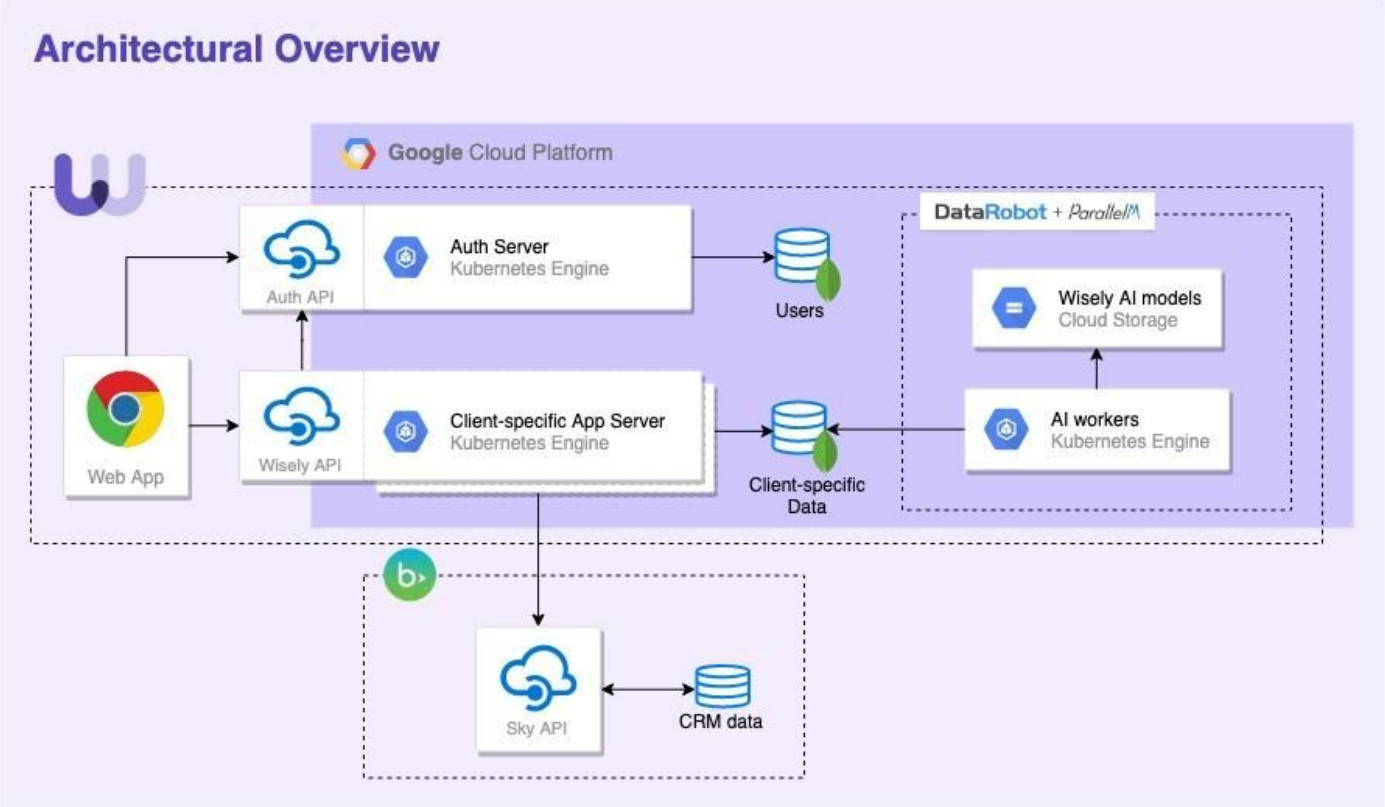
Wisely's on-site Toronto-based engineering team is fully responsible for ongoing development of the product. We only connect to your CRM system through Blackbaud's Sky API giving you complete control over what data can be accessed by Wisely. We then use your data to build AI-powered features designed to help your fundraisers do more with your data, while maintaining data security and privacy. Please see Wisely's Privacy Policy for more information on how data your data is stored and used.

Wisely is a SaaS offering built on top of the Google Cloud Platform (GCP) fully-managed infrastructure, including MongoDB Atlas fully-managed databases hosted in our production GCP instances. We also partner with ParallelM, a DataRobot company and the leader in automated machine learning, to manage our AI/machine learning pipeline on GCP.

Wisely employs many layers of security to help protect our customer's data. This document addresses the following requirements:

- Access Controls
- Data Confidentiality and Privacy
- Processing Integrity
- Physical Security
- Availability

© 2019 Wisely Cloud Inc. All rights reserved. Wisely and the Wisely logo are trademarks of Wisely Cloud Inc.
All other marks are trademarks or registered trademarks of their respective holders.



Access Controls

Users interact with the external interfaces of the Wisely application via a web-based user interface; components required for this interface use the Wisely API which communicates internally with the managed GCP cluster with no external exposure. Any required internet-based communications use TLS 1.2 to protect the confidentiality of the authentication process as well as data in-flight.

Web-based authentication

To log into the application website, users authenticate by providing a username (which is their individual organization email address) and password. The authentication process is handled over HTTPS using TLS 1.2 to the application server. When the user sets their password, it is securely stored in the database pictured above. Before the password is stored, it is hashed and uniquely salted using SHA-512.
The original password is discarded and never permanently stored.

API authentication

All API communications use TLS 1.2 to protect the confidentiality of authentication materials. When interacting with the Wisely API, authentication is performed using a bearer token contained in the HTTP Authorization header.

Authorization

The Wisely cloud system is a multi-tenant solution, but data is partitioned at the client organization level. That is, Wisely stores all organization data under client-specific collections and manages user access control on a per-client basis.

Security Monitoring and Alerting

Wisely uses many security tools to continuously monitor the production GCP/SaaS environment, including Google's Cloud Security Command Center. All system requests are logged, such as web requests, storage bucket access, and user account access.

© 2019 Wisely Cloud Inc. All rights reserved. Wisely and the Wisely logo are trademarks of Wisely Cloud Inc.
All other marks are trademarks or registered trademarks of their respective holders.

Data Confidentiality

Data is secured at-rest using encryption. MongoDB Atlas encrypts all cluster storage and snapshot volumes, securing all cluster data on disk using Server-Side Encryption. On top of file system encryption, all data transferred to and from GCP is encrypted in transit using TLS 1.2.

Wisely will not collect or store your data that is subject to regulatory compliance, specifically HIPAA and PCI or that has a classification that requires specific security controls.

Data Removal

Wisely will automatically remove all data from client-specific collections at the end of the contract agreement if the SaaS agreement has been terminated. Wisely's backup cycle is designed to expire deleted data within six months of the collection deletion. Deletion may occur sooner depending on the level of data replication and the timing of Wisely's ongoing backup cycles.

Corporate Security

Wisely's systems can only be accessed by our whitelisted on-site Toronto-based engineering team.

Disaster Recovery

Wisely leverages fully-managed continuous backups. In the case of a business continuity event, Wisely notifies customers through proper escalation channels, with accountability and responsibility led by our Chief Technology Officer.

Code and Component Security

Every major product release goes through binary static analysis and dynamic analysis. Additionally, Wisely runs vulnerability scans and assessments of third-party components. Wisely's engineering teams triage and address issues as they are identified.

Software Development Life Cycle (SDLC) process

Wisely releases new code to the cloud environment every week, vetted by a formal change management process. All code commits are subject to peer review, automated testing, and manual testing. When testing is complete, changes run in a staging environment prior to deployment to the production cloud.

Physical Security

Wisely is hosted on GCP, and Google's data centers are ISO 27001 certified, and have HITRUST and other certifications. Please refer to GCP's security document (linked below) for details of these certifications.
Google's installs robust surveillance and detection in and around their data centers with robust perimeter security, Closed Circuit Television (CCTV) cameras, multifactor authentication mechanisms, and intrusion detection. Please refer to GCP's Data Center Security document here:
https://www.google.com/about/datacenters/inside/data-security/index.html

For more information on our fully-managed infrastructure's security, please visit:
https://cloud.google.com/security/
https://cloud.google.com/security/infrastructure/design/
https://www.mongodb.com/cloud/atlas/security

© 2019 Wisely Cloud Inc. All rights reserved. Wisely and the Wisely logo are trademarks of Wisely Cloud Inc.
All other marks are trademarks or registered trademarks of their respective holders.