Wodwo Security Documentation

Administration

Administrative interfaces to Wodwo are protected via access lists enforcing VPN login. These interfaces implement unique per-user accounts, strong password enforcement, and multi-factor authentication. Operational processes (e.g., database updates and code changes) are documented, peer reviewed, and tested in a staging environment before being implemented in production.

Administrators monitor vulnerability announcement lists and apply appropriate patches in a timely manner. A list of third-party software libraries is maintained for identification and remediation as needed. Administrators are granted access based on the least privilege principle. Developers do not have direct access to the production environment.

Availability

The application stack is hosted on a highly redundant and distributed cloud infrastructure which reliably provides fault tolerance.

Replication and versioning and have been enabled to allow quick restoration and/or rollback of files. Source code, documentation, and other application resources are maintained in separate systems for disaster recovery.

Prevention

The application design minimizes opportunities for attack by limiting the use of user-provided information. User fields and forms have been configured to allow only appropriate entries on the client side, and all input is then cross-checked on the server side to harden the system against attacks. Even after this cleansing, this information is not used internally as a reference for any particular component.

The dataset creation process only accepts CSV and XLSX files that contain specific headers, do not exceed a reasonable maximum size, and discards any information that does not correspond to those headers. It then sanitizes each record before attempting to match it in the Wodwo database. No data from the original file is used after the dataset is created.

Well-known and peer-reviewed format-specific libraries are utilized for their respective data structure formats instead of custom libraries.

Wodwo implements firewalls to limit available attack surface, and load balancers to minimize the effects of denial-of-service attacks. Penetration testing is performed annually on the system as a whole and on each component as changed.

Auditing

All access to the Wodwo application and systems is logged and regularly audited.
Workflow process logs are maintained and audited for performance monitoring, error tracking, and appropriate usage patterns.

Application errors are forwarded to a notification and tracking system to alert the support team, who will identify and rectify issues in a timely manner.

Wodwo Inc.
506 Carnegie Center Drive, Suite 105
Princeton, NJ 08540

www.wodwo.co
contact@wodwo.co
phone: 855-28-wodwo

Support

While automation can proactively detect many issues, end users play a vital role in noting abnormal behavior. As such, easy access to the support team is offered on every page of the application.

Customer Data

Wodwo does not retain uploaded customer files. The dataset creation process matches records from the customer file to those contained in the Wodwo database, and it generates a list of unique identification numbers for further use in the modeling and order processes. The original uploaded file is then securely deleted, removing both matched and unmatched customer data from the filesystem. Wodwo shall retain ownership of its models and the associated data. Certain artifacts of the Wodwo application process (datasets, insights, model summaries, and ordered products) are licensed exclusively to the client for a single use.

Payment Card Information Compliance (PCI)

Wodwo leverages Stripe for the billing workflow. All PCI-related information is stored only within Stripe, and can only be overwritten, not viewed, from the Wodwo platform.

Data Encryption

All Internet-routed traffic is protected in-flight using TLS 1.2+ encryption.
All storage utilized by Wodwo is protected at rest using AES-256 encryption.

User Management

Wodwo provisions a unique per-user account identified by an email address. User account information may not be shared, transferred or sold to any third party. Passwords must meet minimum complexity requirements and are stored salted and hashed to prevent credential leakage.

Each user account is linked to a company account within Wodwo, and is assigned a permission level within that company:

> User: Can see the results of all other product activity within the company account and a list of users. They cannot see billing-related information, nor make changes to any user account other than their own.
> Admin: All permissions of the "User" and can also manage other user accounts within the company, change plans, and modify address and billing information.
> Owner: All permissions of the "Admin" and has the authority to request closure of the account.