Security FAQ

Authentication

Q: Do you enforce multi-factor authentication?

Observable uses 3rd party authentication providers (Microsoft, GitHub, Google or Twitter) as well as email login through a one-time-password which is emailed to the user. If your users have multi-factor authentication configured with their authentication providers, it will be enforced by Observable.

Q: Do you support SSO/SAML?

We support OpenID Connect with Microsoft and Google. OpenID Connect is a simple identity layer on top of OAuth 2.0.

Personal Information

Q: What personal data do you collect from users?

We collect your information only with your consent in accordance with our Terms of Service. We only collect personal information that is necessary to fulfill the purpose of your interaction with us. Please see our Privacy Policy for more details about what personal data we collect from users.

Network Security

Q: Is all the network traffic handled through HTTPS?

Observable is only accessible over HTTPS and only encrypted HTTPS and websockets (WSS) are used for data transmission. Our commercial certificate is signed by Cloudflare, and we only allow TLS 1.2 and higher for HTTPS connections.

Security Assessments and Compliance

Q: Do you scan for security vulnerabilities?

Our production infrastructure is hosted by Heroku, and is contained within Heroku's secure network. Heroku regularly undergoes penetration tests and vulnerability assessments to ensure that the network remains secure. See: https://www.heroku.com/policy/security.

In addition, we rely on GitHub Enterprise's advanced vulnerability scanning and security alerts. They monitor our codebase and dependencies for vulnerabilities, and issue automated alerts when problems are found. See:
Our software development process prioritizes the patching of vulnerabilities, whether found by automated vulnerability scanning, or by developers during ongoing code reviews.

Q: Do you conduct external (third-party) audits of the service? Are you SOC2 certified?

Not yet.

Data Security

Q: How do you protect user data?

Our user data is entirely hosted on our production systems, which include Postgres databases hosted by Heroku and administered by Observable, and an S3 account hosted by AWS and administered by Observable. None of our user data is transferred to hosted file sharing services.

When users access data from their notebooks, the data does not reside in our systems. It flows from the data source to the user's browser and none of that data is stored in Observable. Please refer to this overview to hear more about how we protect our users' data.

To read more about how the Observable architecture protects your code running in a web browser, please refer to this notebook.

Q: Do you offer an On-Prem solution?

Observable does not offer an On-Prem solution. However, it is still possible to securely connect to data that cannot leave your private network, by installing a database proxy on your network. In this configuration, data travels from the source, through the proxy, and to the user's browser without ever having to leave the network.

We provide an open source Node.js database proxy for self-hosting.

Q: Do you use any sub-processors for data processing purposes?

No.

Q: Does your application enable granular permissions and roles to be created?

In Observable Teams, we allow team owners to assign roles of 'owner', 'editor', or 'viewer' to team members. That defines the overall permissions for users in a team. At the notebook level, team members can control view and edit permissions on their notebooks with individual users on the team or the whole team.

Privacy

Q: Are you GDPR or CCPA compliant?

Not yet. Please see our Privacy Policy for more details.

Operational Security

Q: Do you conduct background checks on employees?

No. It is our company policy to respect the principle of least privilege when designing access controls and administrative tools. For example: all employees have access to notebook metadata, but only support personnel have access to the content of the notebooks. In addition, all personnel are required to sign Confidentiality Agreements to protect customer information.

Q: Describe your security awareness program for personnel

Our employees are currently required to train on our company policies, which include:

- Work Computer Policy: to properly secure employee endpoints
- Secure Software Development Process: which describes how we design, build and deploy our software with security taken into consideration on every level
- Security Incident Management Process: describing the steps and procedures that should be taken if an incident were to occur

To learn more please visit **observablehq.com** or reach out at **sales@observablehq.com**