

The assignment is centered around Conduction, an open-source task management platform. Data processing and querying is done on-device, but raw user tables and data is stored in a remote PostgreSQL server that's either officially hosted and supported or optionally on-prem hosted by the user.

1 | **What are we protecting?**

Because of the open-source nature of Conduction, and the fact that all data processing code is done with the client application, the most important asset to actually protect is any user's data (tasks, perspectives, due dates, etc.).

This means creating a secure pipeline between our servers and that of the clients, that from self-hosted servers and that of their clients, and finally the clients themselves.

The scope of Conduction is has too narrow scope to protect anyone but direct Conduction user's data, including misuses of the client app or API but not including users of a third-party services with indirect API interfaces to Conduction.

2 | **Who are we protecting it from, and what are their motivations?**

2.1 | **Protecting from...**

- Advertisers who may want to advertise based on notes of users
- Foreign companies and groups who are attempting to access privileged information
- Bad actors looking to leverage a "weak-point" in a user's security profile
- Well-meaning but security-unconscious users

2.2 | **Not Protecting from...**

- Organized, state-supported exploits
- Third party authorization and our hosting partners