Technology with Security at Its Core

Aira's infrastructure runs on the global leading cloud platform, Amazon Web Services (AWS). By combining their offering with our expert architecture, we're able to deliver privacy and security while maintaining the conveniences our customers have come to love.

Secure Platform Design

The multilayer security of the platform comes from the Virtual Private Cloud (VPC) within AWS and the TLS protocol that guards all internal and external communication. This ensures our network is not publicly accessible, and all traffic through our private network is secure with respect to our private network as well (via AES 256). The platform is an aggregation of special purpose components, with each component having its own security group. These security groups restrict both access and communication. The gateway acts as the front door to our VPC, and only allows our proprietary communication through (this prevents people from being able to leverage SSH to access servers within our VPC).

With respect to storage, we do not store any payment related information. All credit card related information is handled by Recurly, which is a PCI-DSS level 1 compliant vendor. We store basic profile information behind an Amazon Relational Database security and management system (which restricts access by IP among other criteria), encrypted using industry standard AES-256 encryption algorithm.

Secure Private Network for Customer Hardware

Our service leverages the Horizon Kit, comprises of 2 hardware devices the user carries with them: the phone controller and our Smart Glasses. The Horizon phone controller is a Samsung J7 device that enables the user's communications via AT&T's DTM network (which the public does not have access to). The Horizon Glasses are connected to the phone controller via a USB interface cable. The glasses itself do not hold any firmware and are fully controlled by phone controller. This eliminates the concern around the security associated with losing glasses.

Secure Customer Hardware

The Horizon phone controller is a Samsung J7 device with Android 7 and later, supporting current industry standard security protocols. The device is managed via enterprise grade device management system, IBM MaaS, letting us gain insights, perform actions, set security policies, control hardware/apps and provide privacy remotely. The device ships in Kiosk mode which prevents access to any and every app on the device. The user only has access to Aira. The device is monitored for

encryption levels, root detection, passcode status, device restrictions, installed profiles and security policies. IBM MaaS enables us to locate a lost device and perform wipe of data (no sensitive data is stored on device) and profiles.

Safe Communication and Distribution of Applications for Agents

Agents assist users by using our Agent Dashboard. It is important to note that before the Agent even gains access to dashboard, let alone attempts to download the application, the destination computer must meet the pre-approved specifications of hardware and software. The Agent Dashboard has a secure distribution via an internal tool which leverages authentication and authorization principles before providing the application for secure download. Our software is signed by Microsoft and Apple, such that they are valid when installed (if an agent were to be prompted about untrusted software installation that would immediately flag the binary as invalid). When the application is run, all communication (audio, video, gps, etc.) is secured via TLS. All sessions are securely stored in our Cloud Platform. Each session has restricted access to prevent the dissemination of private information.

Securing data in transit

Aira ensures that all the data as it transmits from the user environment and flows through to our private network is always multilayer protected. The Smart Glasses not only encrypts the streaming video using the latest enterprise standard TLS, but it also ensures the transport is safely conducted through a private VPN Network. The Horizon phone provides a local private network which routes the stream of encrypted data through AT&T's Dynamic Traffic Management (DTM) private LTE network until it reaches our Virtual Private Cloud (VPC). This over the air communication through DTM provides our customers with priority routing (which avoids user congestion through cell towers) and an additional security layer on top of the AES 256 encryption provided by the TLS. Once the data arrives at our VPC in Amazon, it goes through our exclusive gateway with a direct connect into AWS. All communication and routing within our VPC is TLS protected.

Low latency and highly available solution

Our guarantee to our customers is that communication from the time from the user streams the video until the agent assisting views the stream is always less than a second. These latency times a carefully monitored with more than 80% of the streams traversing the system in ⅛ of a second and 99% traversing the system in under ½ of a second. We complement this incredibly low latency with our high availability strategy. By leveraging AWS, we are guaranteed the platform will have a minimum uptime of 99.99% throughout the year. We are able to achieve this performance by having each component in the platform dynamically scale based on user demand.