YOUR PRIVACY, PROTECTED

EDGE DEVICES

Tack and Vista collect data at the endpoint, and store it locally on the device. Data is always encoded, and never available in plain-text format. The only information stored by edge devices are sensor data, so information related to installation location, the client, etc. is never available. Every device is password-protected, and anonymous data collection is available. In this case, data will still be encoded, and is never location-associated.

GATEWAYS

CoolR's Global Hub pulls data from edge devices and transmits it to the Cloud using its own connectivity. Gateway data is stored in the application-specific folder with restricted access, and decrypted data is never stored. Each gateway requires user authentication.

COOLR PORTAL

The components which make up the CoolR Portal communicate internally, restricting external access. HTTPS protocol is used to ensure data encryption during transmission. Multiple security layers protect Cloud data. Firewall rules limit database servers to only be reachable by the app server.

IMAGE PRIVACY

CoolR is committed to preserving privacy and security. The images taken by our devices do not have any identifying information related to location, and image copies of employees/contractors are never stored on local systems without prior consent.

Our devices do not record audio and video, and cameras are inward facing so as to only capture the inside contents of the cooler. Image capturing is not constant, and occurs only when the cooler door is opened. If a partial body image (like a hand reaching inside the cooler) is captured, the image is "destroyed" within 24 hours of transfer outside the store.

Unless an alternate storage location is agreed upon, all data is stored within the U.S. Images are never used for any personal information tracking, only to identify the contents inside coolers and commercial refrigerators.