KEIRTON

Cloud Security Overview
for the Cure Puck

Revision 2

1. Cure Puck Cloud

- **Encryption of messages:** All communications through Cure Puck Cloud are securely encrypted.
- **Access permissions:** Users can finely control who can access their devices and data within their organization.
- **User authentication:** Cure Puck Cloud requires each user to have a verified email address, using an in-built verification system.
- **Server design and access control:** The design of the server system ensures that only authorized users can access devices in your organization's network.
- **Unique device authentication:** Devices are secured with individual OAuth tokens and Product IDs.
- **Proactive monitoring:** Cure Puck Cloud actively monitors for any unusual activity to respond swiftly to potential security threats.
- **Use of TLS standards:** The platform primarily uses Transport Layer Security (TLS) protocols for security. Cure Puck Cloud prioritizes the latest TLS protocols, such as TLSv1.3, but will default to TLSv1.2 if necessary. Older versions like TLSv1 and TLSv1.1 are not supported, and connections using these are automatically terminated.
- **Port usage:** For secured TLS connections, Cure Puck uses port 443, or 9443 as an alternative.

2. Cure Puck Hardware Library

- The Cure Puck library typically establishes a TLS (v1.3) connection between hardware and server.
- Each piece of hardware is authenticated using a 24-byte, base64-encoded OAuth token, changeable through a re-provisioning process.

3. Cure Puck Apps for iOS and Android

- These apps use secure web sockets, opting for TLSv1.3 or TLSv1.2 based on browser compatibility, and implement basic email/password authentication.

- Passwords are encrypted client-side before cloud transfer, ensuring that only encrypted hashes are stored and utilized server-side.
- A security measure limits login attempts, blocking an IP for 10 minutes after five unsuccessful login attempts.

4. Cure Puck Cloud Database Security

- Data transfer between the cloud and database is always encrypted.
- While the database is not encrypted by default, encryption is offered as a paid add-on.
- Cure Puck's service provider currently holds SOC 2 Type 2 certification.

5. Certificates and Ports

- Cure Puck employs Let's Encrypt certificates for TLS, renewing them bi-monthly.
- Standard ports are used: port 443 (or 9443) for TLS and port 80 (or 8080) for plain connections.