Cygnus Reach Security

SECURING REMOTE SUPPORT IMPLEMENTATIONS

Simple Secure Remote Support

Cygnus Reach SDKs streamline the secure integration of remote support features within your applications. While they don't directly secure your entire app, they provide a strong foundation specifically for Cygnus Reach functionality. This frees you to focus on building a great app experience while ensuring secure remote interactions.

SECURE REMOTE SUPPORT FEATURES:

- **Simple Secure Connections:** The SDKs handle the heavy lifting of securing the Cygnus Reach communication channel. This includes robust encryption, secure data storage, and industry-proven authentication protocols.
- **Reduced Security Risk:** Battle-tested security measures embedded within the SDKs and regular platform updates from Cygnus minimize vulnerabilities specific to remote access.
- **Confidence Through Testing:** Rigorous penetration testing of the SDKs ensures a secure foundation for Cygnus Reach functionality within your app.

Remember: The Cygnus Reach SDKs secure the implementation of remote support within your app. It's still crucial to follow best practices for overall app security, including secure coding and data handling within your app logic.

By using Cygnus Reach SDKs, you gain a secure and efficient way to integrate remote support features. This allows you to deliver a trustworthy user experience with reduced development effort.

STANDARD CYGNUS MOBILE & CLOUD PLATFORM SECURITY

APP/MOBILE DEVICE

- **Empowering User Control:** The end user is always in the driver's seat. They initiate the remote session, invite the agent, and have complete control over what features are authorized for access.
- **Proximity Limitation:** The end user needs to be in close proximity to the device in order to connect.
- **Unrestricted Access Blocked:** Public access to your device is strictly prohibited. Only authorized agents invited by the user can gain access.
- **Granular Permission Management:** Users have the power to grant specific permissions for each remote session. This ensures only the necessary features are accessible to the agent, minimizing risk.

SECURE CLOUD

- **Secure Access with API Keys:** Each connection requires a unique Cygnus Reach API key, adding an extra layer of authentication and preventing unauthorized access.
- **Ironclad Data Protection:** All cloud platform traffic is encrypted in transit, safeguarding sensitive information during transmission.
- **User Privacy First:** Cygnus Reach has a zero-tolerance policy for storing end-user personal information within its network. Your users' privacy is paramount.
- **Unwavering Privacy Standards:** Cygnus implements industry-leading privacy protection measures to ensure user data is handled responsibly and in accordance with best practices.

EMPOWERING SECURE BLUETOOTH CONNECTIONS WITH CYGNUS REACH

Bluetooth's ease of use comes with a security responsibility. Developers grapple with finding the right balance: robust security without hindering the user experience.

CYGNUS REACH EMPOWERS DEVELOPERS TO ACHIEVE THIS BALANCE

- **Flexibility for Varied Needs:** Whether you're building a healthcare app requiring top-tier security or a fitness tracker focused on ease of use, Cygnus Reach adapts. Choose from industry-standard security features like multiple encryption algorithms, strong authentication protocols, and role-based authorization.
- **Simplified Development:** The Cygnus Reach protocol streamlines development by providing pre-built security features. This saves you valuable time and resources, allowing you to focus on crafting exceptional app functionalities.
- **Developer Choice in Security:** Cygnus Reach doesn't dictate a single approach. It provides a comprehensive set of security options, allowing you to tailor security measures to your specific application's needs.

THE POWER IS IN YOUR HANDS:

Cygnus Reach empowers you to strike the perfect balance between user experience, data protection, and safety. It provides the flexibility to choose the right security measures for your specific application, without sacrificing development efficiency.

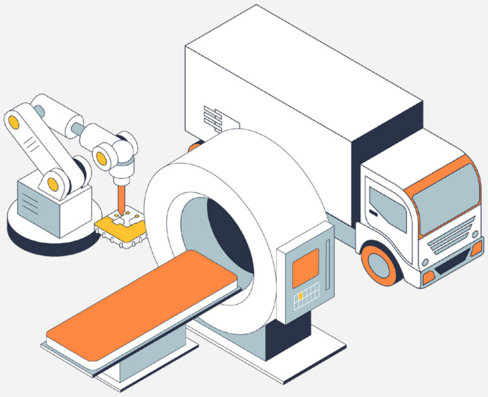
By leveraging Cygnus Reach, you can deliver secure and user-friendly Bluetooth connections within your app, fostering trust with your users.

For questions regarding the security models in the Cygnus Reach Cloud, SDKs, or device connections, please contact **support@cygnustechnology.com**

Standard Device Security

LOWER RISK DEVICES

- Device to Mobile Device BLE security uses industry standards of encryption and authentication keys
    - Mode 1, Level 2 – Encryption only
    - Optional role-based authorization keys can be implemented to secure device configurations and logs at multiple levels
- Proximity to the device is required



Strong Device Security

EQUIPMENT REQUIRING SAFETY CONSIDERATIONS

- Device to Mobile Device BLE security uses industry standards of encryption and authentication keys
    - Mode 1, Level 4, privacy mode enabled – encrypted & authenticated
    - Role based authorization keys implemented to secure machinery features at multiple levels
- Proximity to the machine is required

Example: Role-Based Authorization Keys

STRENGTHEN YOUR APP'S SECURITY WITH ROLE-BASED ACCESS CONTROL

Cygnus Reach empowers developers to add an extra layer of security specific to their app. This is achieved through role-based access control (RBAC) managed within the secure Cygnus Reach portal.

Here's how it elevates your app's security:

- **Granular Permissions:** Define user roles and assign specific permissions within your app through the Cygnus Reach portal. This ensures only authorized users can access sensitive features.
- **Secure Key Management:** Unique encryption keys are generated for each role within the portal. These keys are securely programmed onto devices during provisioning, keeping them protected.
- **Compromise Response:** If a security breach is suspected, compromised keys can be easily revoked and updated within the portal. This swift action helps mitigate potential damage.

By implementing application-level security with Cygnus Reach, developers can create a more secure and permissioned environment within their app, fostering trust with their users.

EXAMPLE ROLE	KEY	EXAMPLE PERMISSIONS
Admin	User-defined	Read/write ALL device parameters, modify Bluetooth security settings, install firmware updates
Technician	User-defined	Read/write SOME device parameters, install firmware updates
End-User	User-defined	Read/write select device parameters