LIFECARE CONNECT
CYBERSECURITY

Lifecare Connect App
Cybersecurity is a core feature in the design of the Lifecare Connect App developed for iOS and Android; each platform securely communicating with the Lifecare Connect Server to display radar data to its users. Through the Lifecare Connect iOS and Android app, authenticated users can monitor real-time system health data, live from one or more connected SCANTER radar systems.

Security by Design principles are embedded into Lifecare Connect App.
Cyber threats and risks are meticulously accessed and security mechanisms and controls such as Code Obfuscation, Encrypted Communication and Access Control are embedded into the two applications to keep the data safe. The mobile application's software implementations have also been tested for known vulnerabilities and flaws regarding the OWASP Top 10 List. In addition to that, OWASP Mobile Application Security Verification Standard (MASVS) at "Checklist" is used to further verify the security controls of the application."

Lifecare Connect Remote Service
With Lifecare Connect Remote Service; remote access to operational radar sites is obtained through an 62443on secure product development. The solution establishes a secure tunnel between the remote client and the radar site through which it allows only authorized and authenticated applications and users to connect to the radar. Two-factor authentication, embedded certificates and time stamped activity logging are some of the controls implemented to make the solution cyber-resilient.

Industrial Specifications
The Remote Connectivity not only complies to international standards for safety and interference it is also both security and Industry 4.0 certified end-to-end according to: NIST SP800-115 for audit process and German BSI Grundschutz and IEC 62443 for evaluation.

IFS: 1602233-QA
Nov-21

TERMA
ALLIES IN INNOVATION

Security Measures	Description
Two-Factor Authentication	Password combined with personal security certificates and optionally extended with SMS code validation
Encrypted communication	The communication from the App to the Connect server is HTTPS enabled leveraging SSL/TLS.
3rd Party Certification	Security audited by 3rd party company: Audit based on NIST SP800-115 and German BSI Grundschutz and IEC 62443 for evaluation.
Time-stamped activity logging	Each log has time stamping in order to prove its integrity making.
Security by Design	Lifecare Connect uses advanced end-to-end encryption (E2EE) and micro-segmentation to ensure data security from your smartphone with the support of VPN connectivity.
Code Obfuscation	Prevent attackers from reverse engineering a software program. Recommended by Open Web Application Security Project (OWASP) to 10.
Access Control	Full control of who can access the App. Both authentication and authorization are performed on the Connect Server.
Device Management	Control who gets access to your devices. Full control of which devices can be accessed by whom.
Validated solution	Lifecare Connect is security certified according to international industry standards.