White Paper: How Remote *Care* Is Designed with Data Privacy & Security

Introduction:

Data security and privacy are primary concerns of LMS and our customers. Remote *Care* is developed to meet strict security standards to protect the instrument data and customer network from unauthorized access. This document examines how the Remote *Care* service was designed with data security and privacy as critical deliverables. Below you will find the requirements for remote service security.

Requirements	Remote *Care* Methodology
Enterprise proven design – When designing cloud-based solution it is critical to select an infrastructure approach that prioritizes platform security, availability and scalability to meet the rapidly evolving technical landscape.	Remote *Care* is built using AWS Cloud Services, a recognized leader in global Cloud solutions for industrial, life-science, consumer and commercial applications. Remote *Care* and instrument diagnostic data are hosted on AWS in Germany with ISO 27001 registration.
Instrument connection flexibility - Support for multiple instrument and connection types without requiring complex or expensive network infrastructure.	Remote *Care* securely supports multiple instruments and connection options. Access to the customer wired or wireless LAN and ability to connect to the internet are the primary requirements.
Rapid deployment – For customers to adopt remote service systems, the security capabilities must co-exist within the customer's current network security model without adding additional costs and overhead.	Only capturing real-time instrument data, the Remote *Care* application uses industry standard secured communication protocols and encryption (TLS1.2 over port 443) for safely managing instrument to cloud connectivity for secure and simple deployment. The Remote *Care* application eliminates the need for VPN and the costs and IT overhead to implement a VPN for the sole use of remote service.
Third-party security firm validation – Official certification by a security audit provides customers with the confidence in the capabilities of the technology and application.	Penetration testing is performed by a 3rd Party vendor on the Remote *Care* infrastructure providing Leica and our customers confidence the service is secure.
Data Protection – The solution must ensure that only authorized connections are possible, and that the data transmitted is properly safeguarded from intercept or manipulation.	Remote *Care* utilizes SSL 256-bit encryption for instrument data in transit and at rest in the AWS cloud infrastructure. Each instrument has a unique security certificate to ensure secure authentication to the service.
Audit Tracking – A robust reporting capability for traceability of actions performed by each user during all sessions.	Remote *Care* includes tools that allow Leica system administrators to audit use of the application including user access, session date/time stamps and actions performed at the instrument level.
User Access Control – The solution should ensure that only approved users have access to the system and that each user only sees the information that is relevant for their responsibilities.	Remote *Care* employs multi-factor authentication (MFA) to validate user access to the service. Furthermore, validated users are controlled by activity and device-based privileges. › Activity based – enables the Leica system administrator to assign and classify Remote *Care* users and define the actions each user can perform. › Device based – enables the system administrator to control the access to only the devices for which a user is responsible. › Only qualified Leica employees have access to customer data.

Network & Data Security Features

- Remote *Care* technology relies on best practice IoT communication mechanisms
- End to end penetration testing performed by a 3rd Party annually
- Remote *Care* agent initiates all communication, so devices do not require public IP addresses and are not visible from outside the firewall
- Certificate based communication, AES-256 encryption, TLS 1.2 protocol with only the outbound 443 port required
- Instrument data is encrypted at rest and in transit to the Remote *Care* application
- Access to Remote *Care* is centrally controlled and authenticated against an enterprise identity system.
- Multi-factor authentication required for user access
- Remote access follows best practices in user/network access (AAA) such as Auditing, Least Privilege, MFA and Groups
- Expensive VPN connections not required

Firewall Configuration

The customer needs to open the Port 443, TCP (Out) to the following addresses:

IoT CoreBase Installation: https://lmsgetiotcertificate.azurewebsites.net/

IoT Updater / IoT Installer download: https://webshare.leica-microsystems.com

IoT Connection:

kafka1.leicams.ls-dhrdigital.com kafka2.leicams.ls-dhrdigital.com
kafka3.leicams.ls-dhrdigital.com a2cim26d8kioks-ats.iot.eu-central-1.amazonaws.com

Communications utilize port 443 and are **outbound** only.
Communications do not use HTTPS – they are binary protocols and use TLS 1.2.

Please note: On-site Proxy Servers are not supported by the application layer

Summary:

Companies throughout the world have recognized the benefits of Remote *Care* and trust Leica to keep their instrument data safe and secure. Through thoughtful development and rigorous on-going testing, Remote *Care* allows customers to achieve their remote service goals – securely and efficiently. If you have additional questions about how Remote *Care* security works? Please contact us at: iot@leicams.com.

CONNECT WITH US!

Leica Microsystems CMS GmbH | Ernst-Leitz-Strasse 17–37 | D-35578 Wetzlar (Germany)
Tel. +49 (0) 6441 29-0 | F +49 (0) 6441 29-2599

www.leica-microsystems.com/remotecare