The Pathology Company

Leica BIOSYSTEMS

APiQ Security FAQ

SECURITY, PRIVACY, AND COMPLIANCE

Security, privacy, and compliance are some of the most common areas that Leica Biosystems receives questions about around Apps. This document aims to answer many of the frequently asked questions about security, privacy and compliance by customers considering APiQ.

WHAT IS THE APiQ HUB?

In the past, configuration of Leica Biosystems software systems has been challenging for customers. By using a turn-key solution, including the APiQ HUB, Leica Biosystems provides a system that is pre-configured and tuned to provide a high quality, highly secure, and highly available system.

IS APiQ SECURE?

Leica Biosystems built the APiQ from the ground up with security in mind. Using this approach means that Leica Biosystems can pre-configure a higher degree of security in the delivered product.

DOES APiQ STORE PATIENT DATA

No, APiQ does not transmit or store any Patient-Identifiable Information (PII) .

WHAT ARE THE CUSTOMERS' RESPONSIBILITIES IN SECURING APiQ?

The Health Care Organization (HCO) that uses APiQ is responsible for these key aspects of IT security:

1. Ensuring secure network connectivity between the APiQ HUB and both Instruments and the Internet. This is because the APiQ HUB uses secure web communications to communicate with the Cloud and connected Instruments.

> In most organizations, this is already in place due to the presence of appropriately configured firewalls

2. Timely installation of security patches for the APiQ HUB, which are delivered by Leica and presented for installation via the web management GUI on the HUB.
3. Provisioning, reviewing and revoking HCO associate access to the APiQ product.
4. Reviewing, approving and revoking mobile device access to APiQ.
5. Physically securing the APiQ HUB.

> The database in the APiQ HUB is encrypted in case of theft or loss. Kensington Lock compatibility is provided to facilitate physical security of the unit.

WHAT ARE LEICA BIOSYSTEMS' RESPONSIBILITIES IN SECURING APiQ?

Leica Biosystems will be responsible for the following key aspects of APiQ IT security:

1. Designing appropriate security controls into the solution.
2. Developing software using a software development methodology that considers security.
3. Organizing independent security testing of the solution and rectifying any vulnerabilities that are identified.
4. Scanning software that will be delivered to customers for malware prior to release.
5. Security patching and securely configuring the software components of APiQ.
6. Providing oversight and governance of service providers such as Microsoft that provide services that support the APiQ solution.
7. Running security processes, such as re-validation of administrator access, aligned with industry standards such as ISO 27001.
8. Responding to reports of security vulnerabilities in the APiQ Product.

APiQ

HOW IS APiQ HUB SECURITY ACHIEVED?

The APiQ HUB is securely configured by default and uses a minimal amount of software needed to perform needed functionality. Only required networking services are run on the APiQ HUB and needed ports are opened. This approach results in a minimal attack surface and reduced attack vectors.

IS THE APIQ SOFTWARE DEVELOPED WITH SECURITY IN MIND?

The APiQ software development life cycle incorporates activities, coding standards and processes which have been put in place to mitigate the top ten security threats as identified by the OWASP Foundation (https://www.owasp.org). Leica Biosystems has a well developed software development methodology and quality management system.

CAN THE HUB BE ACCESSED BY LEICA BIOSYSTEMS WITHOUT THE CUSTOMER EXPLICITLY GRANTING ACCESS?

No.
If RemoteCare access is enabled for Leica Biosystems, the customer can coordinate access to the APiQ HUB upon request. The HCO has the ability to disable RemoteCare access entirely.

CAN I MAKE CONFIGURATION CHANGES TO THE APiQ HUB?

The APiQ HUB is configured, tuned, and secured by Leica Biosystems and cannot be modified by the customer. Customers cannot login to the APiQ HUB operating system; all changes to the HUB must be made through the web interface.

HOW IS THE APIQ SOFTWARE PATCHED?

All APiQ software patches are provided by Leica Biosystems. APiQ HUB software patches can be installed by the HCO through the Administration web interface.

LEICA BIOSYSTEMS CLOUD

WHERE IS APiQ'S CLOUD HOSTED?

APiQ'S Cloud is hosted in Microsoft Azure. Azure offers a reliable platform for software services used by thousands of businesses worldwide. Azure provides services in accordance with security best practices and undergoes industry-recognised certifications and audits. This means that APiQ customers benefit from Microsoft's ongoing commitment to security practices for stored assets. For further information, refer to the Microsoft Azure at http://azure.microsoft.com/en-us/support/trust-center/compliance/.

WHERE DOES CUSTOMER DATA RESIDE?

Customer data is stored in Microsoft Azure and Leica Biosystems designates the physical region in which an individual customer's data will be located. Data replication for data objects is done within the regional cluster where the data is stored and is not replicated to data center clusters in other regions. For the United States and Canada, Leica Biosystems operates APiQ out of the United States. Example: By default, all data from APiQ customers in the United States will have their cloud data stored in the Azure data center in the United States and that data will not be transferred to data centers outside the United States.

WHAT ARE LEICA BIOSYSTEMS' RIGHTS TO CUSTOMER DATA?

APiQ Cloud customers retain control and ownership of their data. Please review Leica Biosystem's Terms of Use and End-User License Agreement for more details, these can be found at www.APiQ.com.

HOW DOES THE APiQ CLOUD ISOLATE CUSTOMER DATA?

All data stored by Leica Biosystems on behalf of customers has strong tenant isolation security and control capabilities. APiQ Cloud storage utilizes Azure Storage which provides advanced data access controls.

WHO CONTROLS THE APIQ DATA CENTERS?

For the parts of APiQ deployed in Azure, Microsoft controls the physical components. To help customers better understand what controls Azure have in place, and how effectively they are operating, Azure publishes a Service Organizational Controls (SOC 1), Type 2 report (http://azure.microsoft.com/en-us/support/trust-center/compliance/) with controls defined around Azure as well as detailed physical security and environmental controls. These controls are defined at a higher level of specificity that should meet most customers needs.

DOES THE APiQ CLOUD SUPPORT ENCRYPTION?

Leica Cloud encrypts data in transit using SSL.

SUPPORT AND MAINTENANCE

WILL LEICA BIOSYSTEMS BRING APiQ CLOUD SYSTEMS DOWN FOR MAINTENANCE?

APiQ Cloud is implemented in such a way as to virtually eliminate downtime. The services should be accessible and reachable during new deployments due to the use of A/B environments and other mechanisms that allow for live-cutover with no externally visible downtime.

WHO IS RESPONSIBLE FOR PATCHING APiQ CLOUD?

Leica Biosystems is responsible for patching our own software and applications running in Azure. Microsoft is responsible for patching their guest operating systems (OS), and is responsible for patching systems supporting delivery of Azure services such as the hypervisor and networking services.