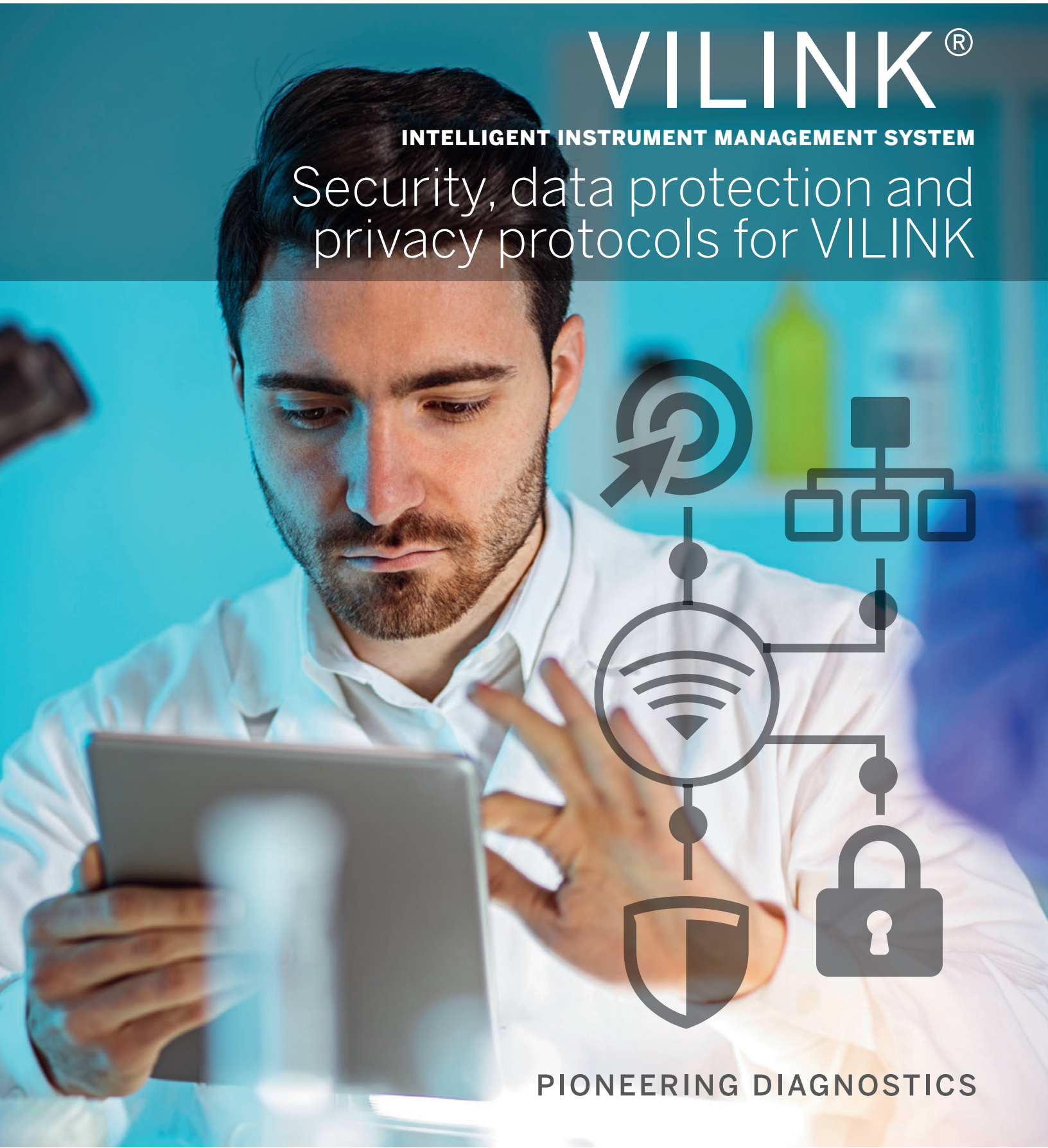
BIOMÉRIEUX

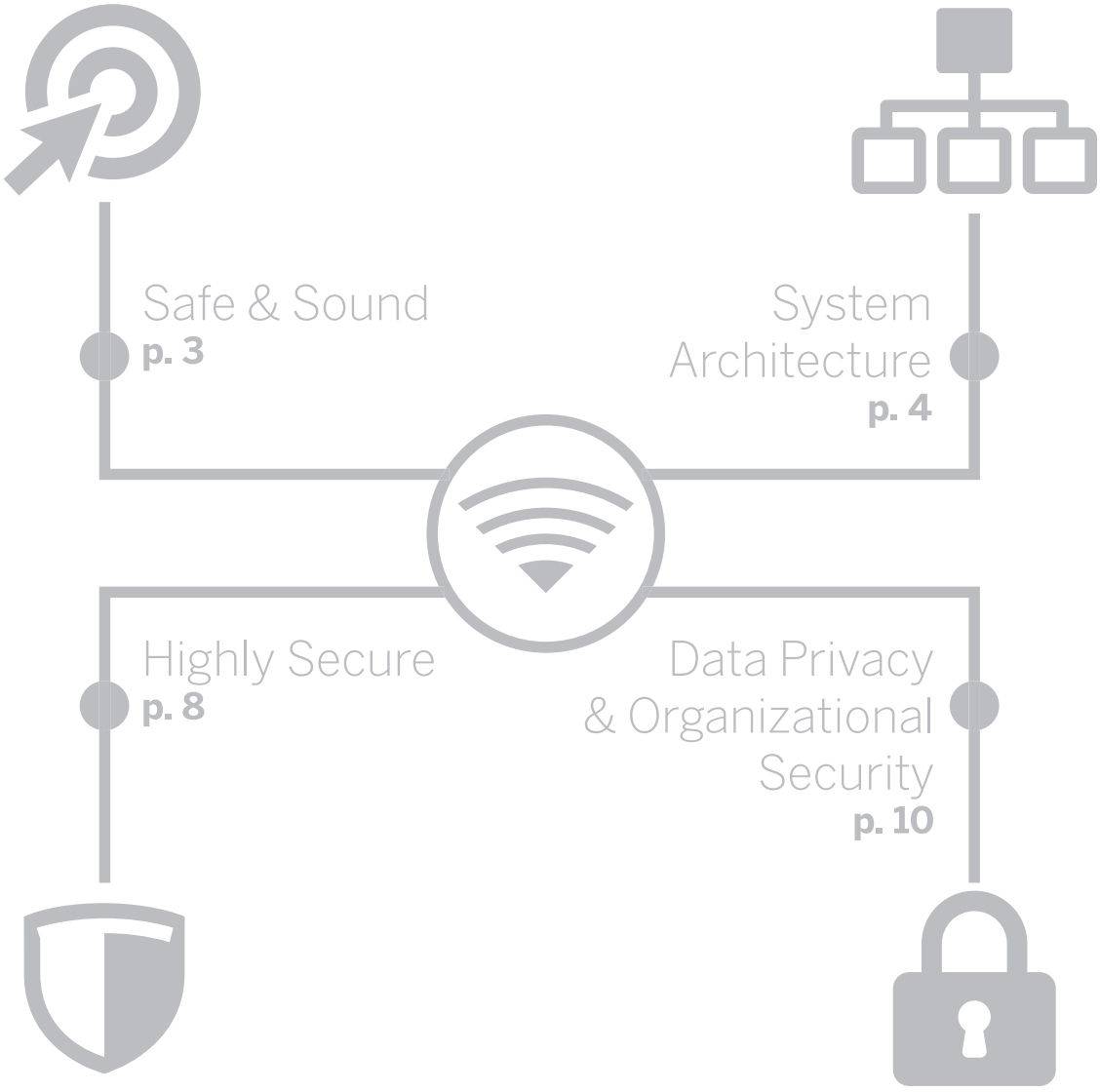
VILINK®

INTELLIGENT INSTRUMENT MANAGEMENT SYSTEM

Security, data protection and privacy protocols for VILINK



PIONEERING DIAGNOSTICS


Safe & Sound
p. 3
System Architecture
p. 4
Highly Secure
p. 8
Data Privacy & Organizational Security
p. 10

Safe & Sound

VILINK® is a highly-secured modular solution that is firewall-configurable and compatible with your organization's security systems. VILINK provides a direct connection between bioMérieux's technical support representative and your systems, it features full traceability and data security via user-approved access and SSL-based encrypted communication.

VILINK enables our service support teams to offer real-time troubleshooting and operator training at your request, reducing downtime and improving efficiency in your laboratory by providing:

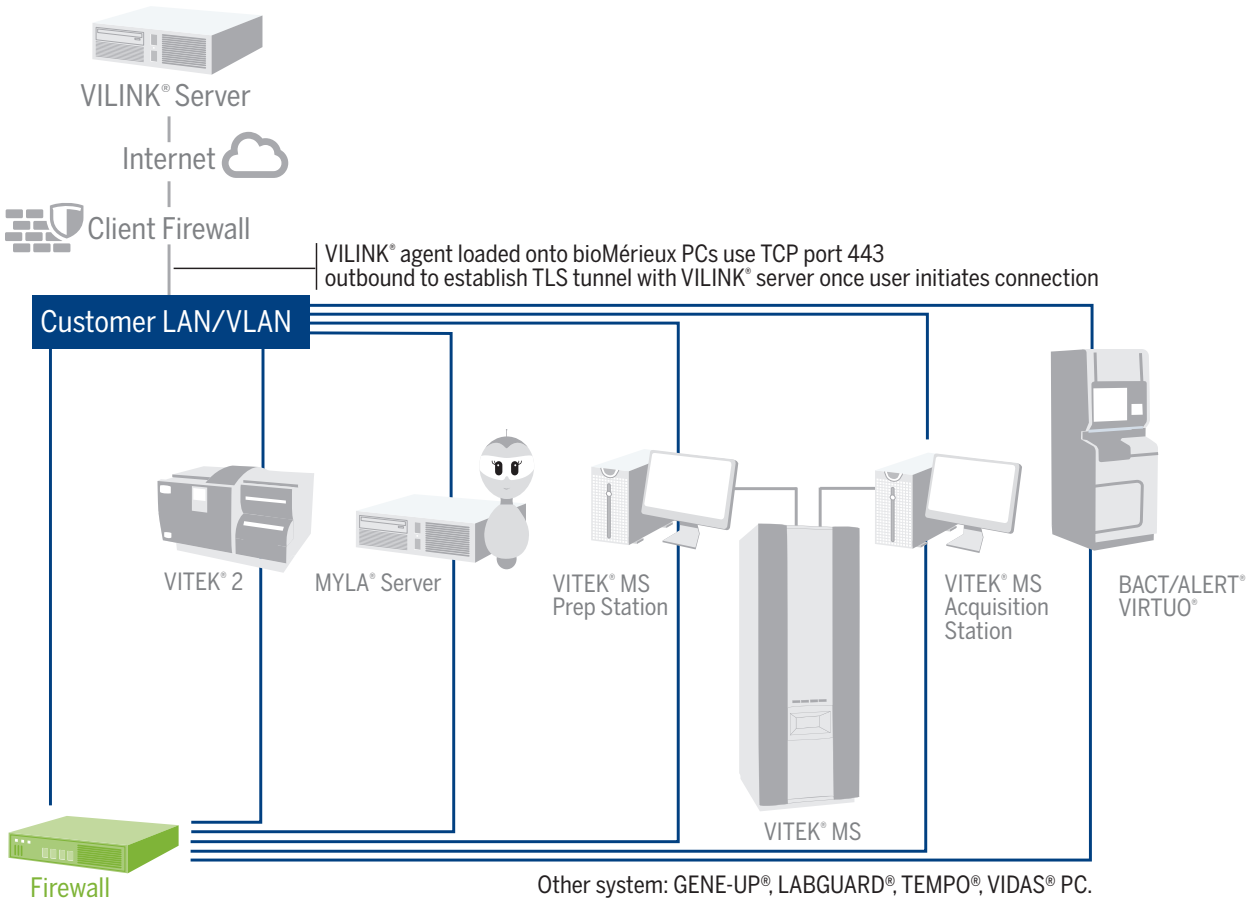
- Remote technical support
- Remote software updates
- Replacement of analog modem technology
- Instant access to new software updates
- Flexible installation options for connecting instrument computers:
  - Local integration through facility's network
  - Isolated internal Local Area Network through bioMérieux's firewall

bioMérieux's security principles:

- We preserve the integrity of your patient data
- We only trace user activities and access to maintain regulatory compliance
- We embrace flexibility to promote autonomous business practices

System Architecture

VILINK® software is powered by Axeda® Corporation/PTC, which provides advanced cloud-based services to manage connected products and equipment. Axeda has excelled in the industry through holding rigorous security standards in the design and operation of its services, like VILINK. VILINK servers are hosted in the US to meet customers needs.



For either option, will need to open up TCP Port 443 outbound connection on your firewall of the following:
- https://US.VILINK.BIOMERIEUX.COM (35.168.64.228)
- https://USEAST1.GAS.VILINK.BIOMERIEUX.COM (35.171.200.102)
- https://USWEST1.GAS.VILINK.BIOMERIEUX.COM (92.13.143.248)

For the full list of VILINK compatible systems, please contact your local bioMérieux representative.

Recommendation

In efforts to promote the security of the laboratory network, bioMérieux recommends connecting instruments on a configured firewall or router with one network socket, and a static IP address, or a reserved DHCP IP address.

Outbound information

The combination of VILINK functionality and our remote technical support capabilities creates a full service support offering. VILINK is non-invasive and never enters your network.

VILINK is installed locally and only sends device-relevant service data, so you will never have to accept incoming connections, and addresses will never be revealed outside the network. VILINK agents can also be configured with FIPS mode enabled, which imposes the strictest security standards (often required in government settings).

Firewall-friendly

VILINK's patented Firewall-friendly™ technology provides two-way communication based on Web Service standards, including Hypertext Transfer Protocol (HTTP), Simple Object Access Protocol (SOAP), and eXtensible Markup Language (XML). All outbound communications are initiated using the HTTPS protocol exclusively on port TCP 443.

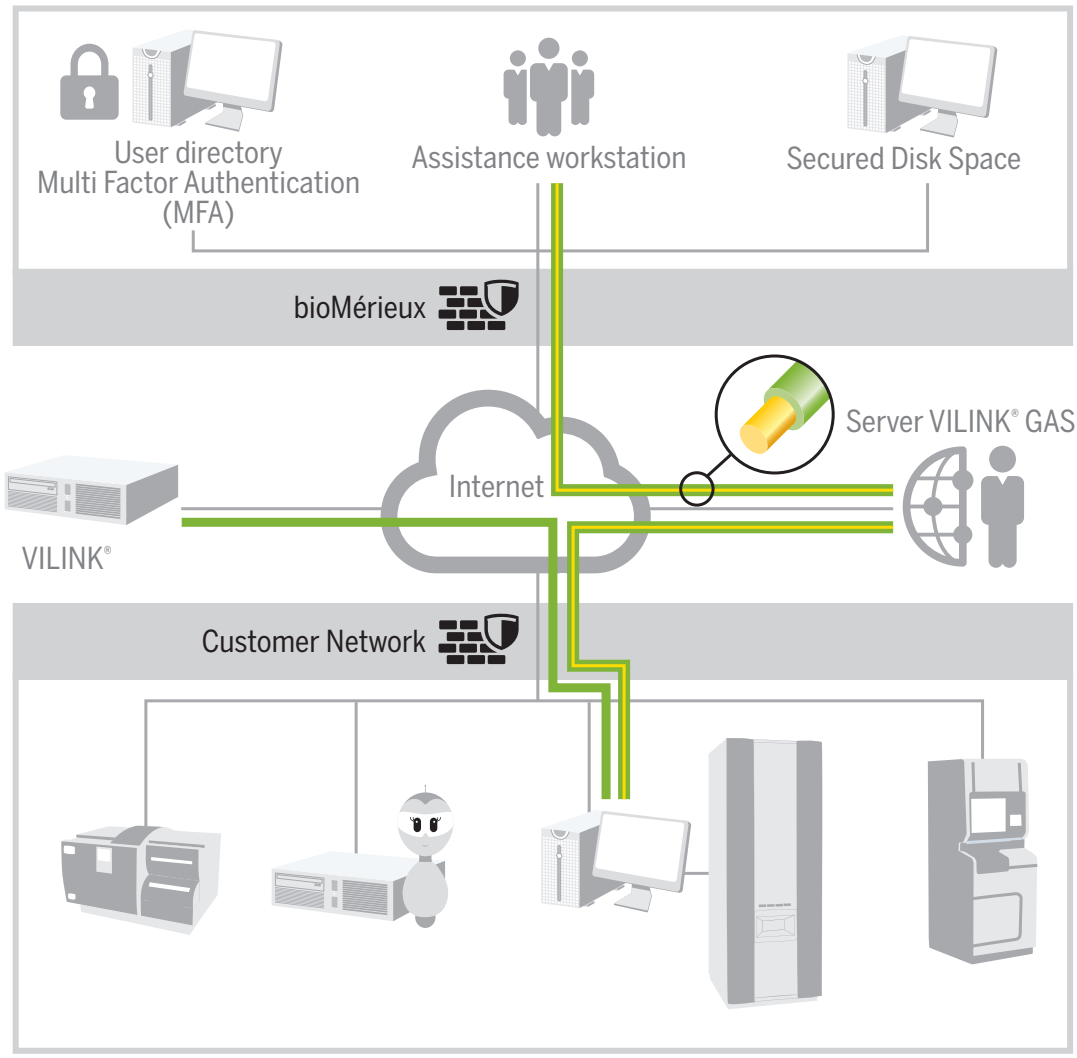
Remote access

When remote access is required, the VILINK support user connects to the VILINK server with their credentials and selects the system they want to access, creating a secure tunnel (based on HTTPS) between the help desk and your bioMérieux commercial system.

The remote user uses validated tools (UltraVNC, Teamviewer®, SSH, RDP) to request remote access, which you can choose to accept or reject. All communication and transferred data goes through the VILINK secure tunnel.

To optimize the remote support experience, we use the Global Access Server (GAS) on TCP port 443. The VILINK server uses the commercial system's nearest GAS server, and if that doesn't work will use the next nearest server.

Your Firewall and Proxy must enable access to the GAS servers on the HTTPS (TCP/443) port. A list of GAS servers is available at https://us.vilink.biomerieux.com/install.



GAS: Global Access Server

Teamviewer® Remote Access

Teamviewer software can be used to improve the speed of remote access, without compromising on security.

You can use:

Teamviewer interface within a VILINK® TLS tunnel so using the AES 256 bits encryption

OR

Teamviewer Direct Mode using the Teamviewer infrastructure. To enable this method you will have to allow the traffic on the tcp port 443 or tcp port 5938 to the domain *.teamviewer.com or on a specific list of IP addresses to be provided on demand

In this Teamviewer Direct Mode configuration, the security features are using the following:

- Whitelist to protect access to commercial systems only to bioMérieux accounts and trusted devices
- RSA Public / Private Keys exchange and AES 256 bits session encryption
- Specific login and password for establishing the Teamviewer session

- Use of Teamviewer is limited to valid VILINK sessions
- By default, the Teamviewer account is inactive and only activated during a VILINK valid period at the end of session. Teamviewer is certified SOC2, ISO9001 and helps you be HIPAA compliant.

Automatic monitoring

Depending on which bioMérieux commercial system VILINK has been installed on, it is possible to automatically monitor the system's computer and devices (instrument, network, or signalization device). Monitoring focuses on technical information such as RAM size, disk-filling ratios, log files, and instrument sensor values. This allows bioMérieux to detect or anticipate variations that may have an impact on the bioMérieux commercial system. Technical information that enables system support is the only information that will be uploaded onto the VILINK server. Information related to patients or biological results will not be uploaded.

Options

You can choose to:

- Have a report on remote accesses of your systems mailed to you (the remote intervention report)
- Authorize service support teams to perform file transfers
- Enable automatic monitoring of your bioMérieux commercial systems
- Retain full access control with the Axeda Policy Server option (see next)

The Axeda® Policy Server (option that establishes and enforces device security and data privacy policies):

The Axeda Policy Server enables your IT administrators to establish and enforce the privacy policy for all of your devices in a single place.

The software application resides on your network, providing a comprehensive and granular set of permission settings that continuously govern behavior, and applies to every kind of Axeda activity, including handling remote diagnostics, sending software upgrades, retrieving log files, running sessions, and executing commands and scripts.

Control can either be automatic, based on the set policy, or configured to notify you that an action request is pending. Policies can also be scoped to time windows and to particular remote users.

Easily Managed User Authentication and Access Control

User access control is addressed through activity-based access control and device-based access control, combined in a wide variety of ways to allow users to do their jobs effectively while protecting access to sensitive information:

1. Activity-based access control enables the system administrator to assign and classify users in Axeda, and define the activities that can be performed. Each user group is given controlled access at the Axeda application, page, and function levels.
2. Device-based access control provides a method for defining the specific devices visible to each user group. This method of control limits the view of device information to only those devices for which a user is responsible.

User and Application Security

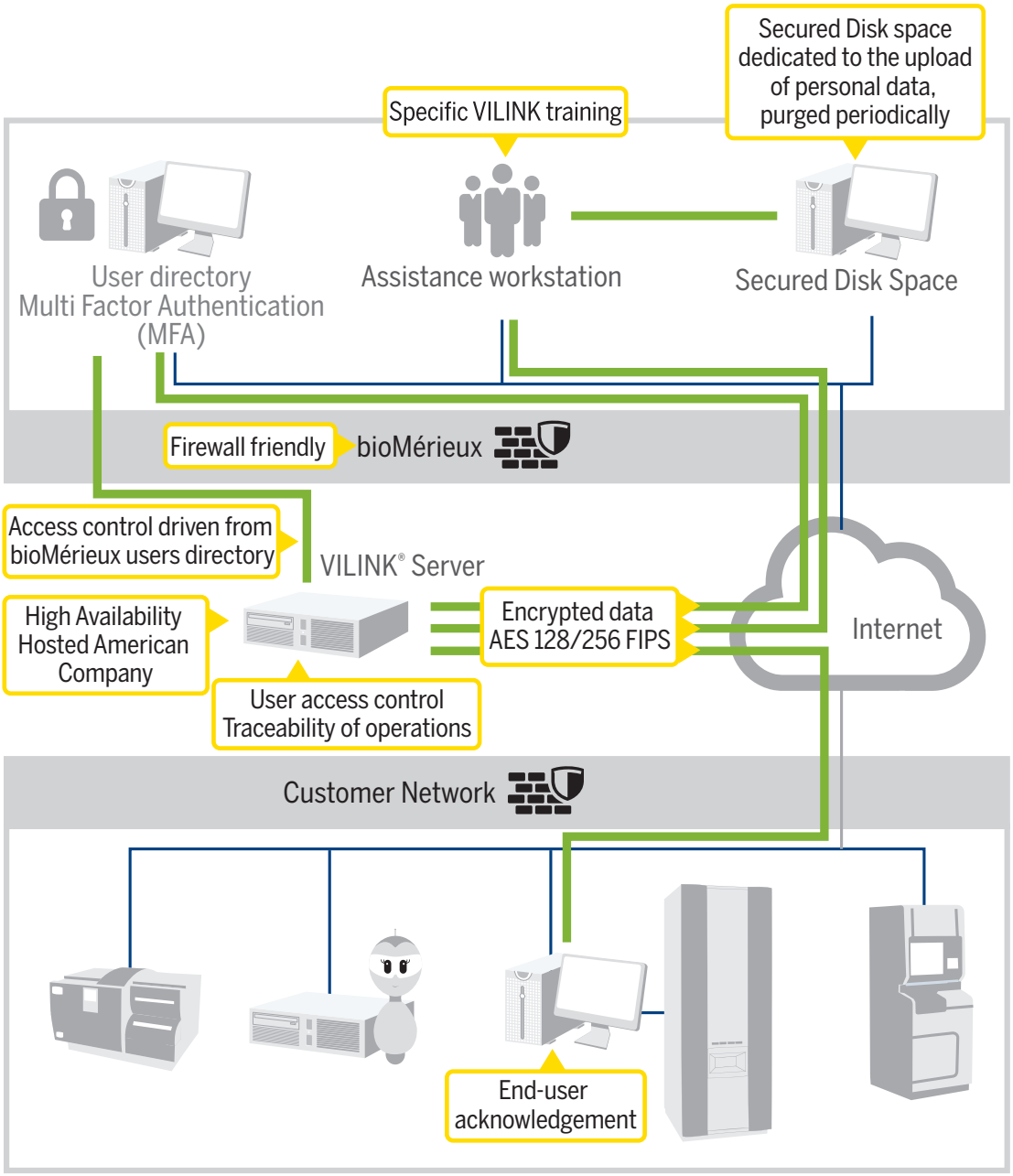
The Axeda Policy Server supports its own internal user store, or it can connect to any Microsoft® Active Directory® (AD) server. This allows end-user IT departments to have centralized control via their normal operating procedures in order to control who manages policies and administers the Axeda Policy Server.

Automatic group synchronization sets roles within the Policy Server based on the AD group membership.

Highly Secure

bioMérieux VILINK® is a highly secured solution using a communication encrypted in AES 256 bits. An acknowledgment on the customer side is required to approve the remote access, and only trained users can use the VLINK solution.

The system offers intentional granular control over user access (attend, unattended, or one-time), and can also offer easy-to-use audit and tracking capabilities.



About the VILINK server

- The VILINK server is hosted in a highly-controlled protected area and is continuously controlled and policed in order to meet both our own high security standards and applicable regulations.
- All server accounts for bioMérieux users are managed by a robust security policy, with encrypted communications established through HTTPS using a 2048 bit RSA certificate. The only protocol allowed through HTTPS at this level is TLS.
- Audit logs record all VILINK user activity (remote sessions, files transfers, etc.) and are maintained on the VILINK server.
- The VILINK server is continuously maintained at a high security and availability level, using the most appropriate and up-to-date security tools (e.g., security scanners) to ensure compliance with best practices in monitoring and penetration testing.

Only PCs connected to trusted LANs are allowed to connect to the VILINK servers (through an IP Filtering).

Connections to the VILINK server

All Commercial Systems connected to bioMérieux VILINK communicate with the VILINK Server through an SSL tunnel (AES 128/256 bits encryption). Every remote session and file transfer goes through this TLS tunnel, protecting any exchange against unauthorized access.

Security configuration

bioMérieux strongly recommends that customers install anti-virus software (supporting Microsoft Windows) on all bioMérieux Commercial Systems, and apply regular operating system security updates. Please see the documentation provided with your bioMérieux commercial system relating to the use of anti-virus and operating systems security updates.

Data Privacy & Organizational Security

bioMérieux has implemented a rigorous data privacy and security program to ensure compliance with all relevant privacy laws during the operation of our software. This program includes, but is not limited to:

1. Assessing and implementing the regulations and standards applicable to the healthcare domain.

2. Gaining your formal agreement before implementing remote access to your network and instrumentation.

3. Implementing a procedure to guard against any data breach in the event of systems being refurbished or swapped over by systematically removing hard drives containing patient data.

4. Limiting user's access to information and information systems in line with their role in the organization, as part of a comprehensive security management system.

5. Screening (when authorized by local regulation) of the personnel accessing patient information.

6. Training personnel who may have access to patient data on internal policies and procedures.

7. Implementing physical security measures to ensure that unauthorized users can not enter bioMérieux premises. These measures include restricting physical access to data servers and data-hosting environments.

8. Complying with password security standards to ensure that authentication can not be easily compromised.

9. Encrypting access to patient data on laptops used by bioMérieux personnel.

10. Protecting connected systems on bioMérieux network from external security vulnerabilities through a combination of hardware firewalls, antivirus software, intrusion prevention systems, and regular Microsoft security updates.

11. Monitoring events at the remote service in order to provide sound and other recordings for optimal quality control.

To follow these security principles, bioMérieux – acting with the support of security experts – regularly performs penetration tests, security assessments, and regulatory audits (e.g., comply with HIPAA).

Local data privacy and security regulations

The system's features have been designed in compliance with applicable local data privacy and security regulations.

bioMérieux, Inc.• 100 Rodolphe Street • Durham, NC 27712 • USA • Tel.: (800) 682 2666 • Fax: (800) 968 9494
www.biomerieux-usa.com