BIOMÉRIEUX

BIOFIRE® SPOTFIRE®

CYBERSECURITY

PIONEERING DIAGNOSTICS

CYBER SECURITY

A SET OF PROACTIVE MEASURES (CYBERSECURE BY DESIGN), SURVEILLANCE AND CORRECTIVE MEASURES.

Cybersecurity is now integrated as soon as possible in the design of our products. Supported by our partners and experts in cybersecurity and data privacy, bioMérieux has implemented a Secure Development Lifecycle that ensures Security and Privacy by Design.

Learn more: https://www.biomerieux.com/corp/en/our-offer/cybersecurity.html
In case of specific questions, please e-mail PrivacyOfficer@biomerieux.com

SURVEILLANCE

- For every new BIOFIRE® SPOTFIRE® release, penetration tests are performed by external companies to scan for new vulnerabilities and threats.
- All vulnerabilities are assessed (impact/criticality) and corrected in a patch if relevant.

EXPERTISE

SUPPORT BY SECURITY EXPERTS

- Skilled staff, experience, and proven coding methodology in development of sensitive platforms (Department of Defense, Space industry).
- Recognized as key leaders in cybersecurity.

PROACTIVITY

- BIOFIRE® SPOTFIRE® is developed and hardened following industry standards.
- A cybersecurity risk assessment is performed prior to each BIOFIRE® SPOTFIRE® software release. Each release integrates cybersecurity updates.
- This cybersecurity risk analysis and best practices are used as an input to BIOFIRE® SPOTFIRE® development and architecture design.

BIOMÉRIEUX

SECURITY FEATURES	BIOFIRE® SPOTFIRE® SYSTEM
Automatic Logoff	The system automatically logs off users based on a configurable period of inactivity.
Audit Controls	Audit Trail records cannot be deleted, are time stamped, and can be exported.
Authorization	The system leverages Windows user rights management which enables role-based access control. Applications are designed to run in non-administrative operating system accounts to prevent tampering.
Configuration of Security Features	The system enables authorized users to configure user privileges for various system functionalities, such as modifying instrument configuration, audit trail, and user management.
Cyber Security Product Upgrades	bioMérieux performs postmarket monitoring and patching of potential vulnerabilties.
Health Data De-Identification	Health data are encrypted for backups and for support purposes.
Data Backup and Disaster Recovery	The system enables authorized users to automate backups and retention settings, as well as configuring data backups in a password protected format and stored on a local network or server. The system can be restored with the assistance of bioMérieux support.
Malware Detection/Protection	Microsoft Windows Defender anti-virus software is installed by default on the system. Other anti-virus software of choice can be installed to fit the security policies that are in place.
Third-Party Components in Product Lifecycle Roadmaps	bioMérieux monitors components for emerging vulnerabilities and issues product updates as needed.
System and Application Hardening	bioMérieux conducts independent third party testing of the device operating system and network settings, including active ports and services.
Security Guides	bioMérieux publishes technical and architectural guidance for the secure deployment and configuration of devices, including security whitepaper, MDS2, and SBoM.
Transmission Confidentiality	The system can be configured with optional connectivity settings. Please refer to program specific documentation for details.
Other	The system runs Windows 10 Enterprise LTSC.

GDPR

HIPAA COMPLIANT

bioMérieux Privacy Statement

The protection of personal data and respect of privacy are fundamental rights derived from the Universal Declaration of Human rights of 1948. bioMérieux is committed to protecting the confidentiality of the personal data of its employees and stakeholders.

Many countries have tightened regulations restricting the use and disclosure of personal data (e.g.US HIPAA Federal law, EU GDPR). These laws require companies to take steps to ensure the confidentiality, integrity and availability of this kind of data. bioMérieux deployed a compliance program regarding regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 which has entered into force in May 25, 2018 (GDPR) as well as national French laws.

bioMérieux has officially designated a Data Protection Officer (DPO) to the French Data Protection Authority (CNIL) to control and ensure compliance of the Company with this regulation.

Product availability varies by country. Please contact your local bioMérieux representative for details.

bioMérieux S.A.
69280 Marcy l'Etoile • France
Tel.: + 33 (0)4 78 87 20 00 • Fax: +33 (0)4 78 87 20 90
www.biomerieux.com • www.biofiredx.com

Manufactured by:
BioFire Diagnostics, LLC
515 Colorow Drive, Salt Lake City
UT 84108, USA

PIONEERING DIAGNOSTICS