BIOMÉRIEUX

BIOFIRE® SPOTFIRE®
Industrial Applications Software

Cybersecurity

Your Ally in Advancing Quality

PIONEERING DIAGNOSTICS

CYBERSECURITY BY DESIGN

BIOFIRE® SPOTFIRE® Industry delivers automated, one-hour nucleic acid testing that's easy to use by anyone, anywhere at any time. It helps pharmaceutical manufacturers reduce time to result, reduce labor costs, and meet regulatory requirements with effortless data integrity. To help ensure compliance with the highest cybersecurity standards, bioMérieux developed the BIOFIRE® SPOTFIRE® Software* using a rigorous cybersecurity-by-design framework.

SURVEILLANCE

- BIOFIRE® SPOTFIRE® Software* is scanned for cybersecurity vulnerabilities using an external reference tool. All vulnerabilities are assessed (impact/criticality) and corrected in a patch if relevant.
- A cybersecurity bulletin is issued internally.

EXPERTISE

- Either at rest or in transit, bioMérieux enforces data protection by implementing security features following current standards such as role-based access control, malware protection, or backup and restore processes.
- For every new major BIOFIRE® SPOTFIRE® Software* release, penetration tests are performed by external companies to detect new vulnerabilites.

PROACTIVITY

- Development and maintenance of BIOFIRE® SPOTFIRE® Software* are perfomed following a secure development lifecycle integrating mandatory security activities and in compliance with regulation such as 21 CFR Part 11.
- A cybersecurity risk assessment is perfomed before each major BIOFIRE® SPOTFIRE® Software* release to ensure safety, security, and privacy.
- Upgrades are released for BIOFIRE® SPOTFIRE® Software*, meaning that the latest features and cybersecurity improvements are always made available for bioMérieux's customers.

How does BIOFIRE® SPOTFIRE® Software* address compliance following the highest international standards?

Benefits	Requirements	SPOTFIRE® Software v1 Feature
Authentication & Authorization	Automatic logoff	The BIOFIRE® SPOTFIRE® Software* software forces automatic logoff after a customizable period of inactivity.
	Authorization	BIOFIRE® SPOTFIRE® Software* software leverages Windows user rights management and built-in Software Accounts Authorization, which enables enhanced role-based access control as well as various permission options. BIOFIRE® SPOTFIRE® Software* applications are designed to run in non-administrative operating system accounts to prevent tampering.
	Person Authentication	There are two types of person authentication: operating system and BIOFIRE® SPOTFIRE® Software* • Operating system: Authentication is done through the local machine Windows password policy. • BIOFIRE® SPOTFIRE® Software*: Person authentication is done through the local software policy or LDAP/s.
	Configuration of Security Features	There are two levels of password strength options which can be configured according to the security policy of the customer.
Availability	Network Controls	BIOFIRE® SPOTFIRE® Software* implements network controls through Windows Firewall configuration, restricting traffic only to specific ports and services.
	Malware Detection/ Protection	Microsoft Windows Defender anti-virus software is installed by default on the system. The customer can also install their coporate anti-malware solution, and apply their own security policy.
Data	Classification(s) of Data Stored	• BIOFIRE® SPOTFIRE® Software* can store personal data like usernames. • To the extent the information contained in any fields populated by the operator is personally identifiable information, such information is displayed and stored on the System.
	Data Integrity and Authenticity	The system includes features to prevent database tampering.
	Data Backup and Disaster Recovery	BIOFIRE® SPOTFIRE® Software* system enables authorized users to perform manual and automatic data backups in an encrypted format and store them on removable or mapped drives. The system can be restored to a prior date with the assistance of bioMerieux support.
	Transmission Confidentiality	For data confidentiality, data is protected using authentication.
	Transmission Integrity	Data is protected with secure, encrypted connections using trusted TLS 1.2 technology.
Audit	Audit Controls	Audit Trail records cannot be deleted, contain a date and time stamp, and can be exported.
	Regulatory Compliance	BIOFIRE® SPOTFIRE® Software* is designed to support 21 CFR part 11 compliance.
Maintenance	System and Application Hardening	Cybersecurity risk assessments, penetration testing, vulnerability monitoring, and manual code review are performed and vulnerabilities appropriately remediated as part of the secure Software Development Lifecycle (SDLC) to ensure the system and application are hardened.
	Cybersecurity Product Upgrades	BIOFIRE® SPOTFIRE® Software* will receive updates as needed to remediate uncontrolled security risk.
	Third-party Components in Product Lifecycle Roadmaps	Software Composition Analysis is performed to facilitate Software Bill of Materials (SBOM) generation and to identify libraries and third-party components utilized to ensure all components and libraries stay up to date.
Other	Security Guides	A detailed Product Security Technical Whitepaper is available for the BIOFIRE® SPOTFIRE® Software*.
	Windows Version	Windows 10 IoT Enterprise 2019 LTSC Version 1809

** Dedicated to Industrial Applications use*