BIOMÉRIEUX

BIOFIRE® FIREWORKS™
CYBERSECURITY

PIONEERING DIAGNOSTICS

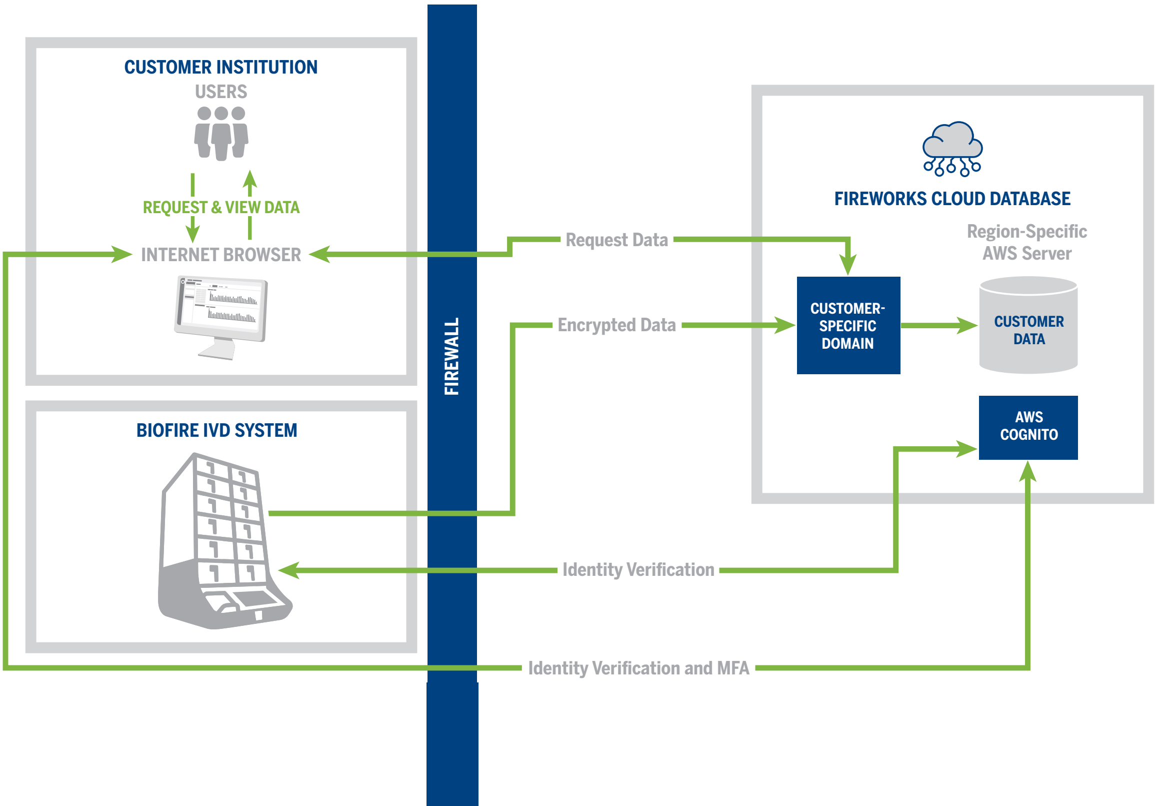
CYBER SECURITY

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 systems and software 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

BIOFIRE® FIREWORKS™ securely transmits BIOFIRE® System data to a unique domain address where it is stored alongside all of your institution's data. Authorized users can then access data from compatible internet-capable devices.



SURVEILLANCE

- For every new BIOFIRE® FIREWORKS™ 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.

- FIREWORKS leverages the constant vulnerability and threat monitoring services provided by Amazon Web Services (AWS).

EXPERTISE

CYBERSECURITY RISK ANALYSIS

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

- Recognized as key leaders in cybersecurity.

PROACTIVITY

- FIREWORKS is designed, developed, and implemented following industry standards and regulations utilizing the Secure Development Lifecycle to ensure safety, security, and privacy.

- A cybersecurity risk assessment is performed prior to each FIREWORKS release.

- The FIREWORKS software updates itself automatically, meaning you always have the latest features and cybersecurity improvements.

SECURITY FEATURES	BIOFIRE® FIREWORKS™
Person Authentication (&MFA)	FIREWORKS uses Amazon Web Services (AWS) Cognito to store user credentials and configure security policy. FIREWORKS enforces Multi-Factor Authentication (MFA) through Time-based One Time Password (TOTP).
Authorization	FIREWORKS leverages role-based access control.
Automatic Logoff	FIREWORKS automatically notifies users after 15 minutes of inactivity. If no action is taken, FIREWORKS will automatically log off the user.
Audit Controls	FIREWORKS logs actions taken by users with AWS CloudTrail. Analysis of audit logs for suspicious activities is performed by AWS GuardDuty.
Health Data Storage Confidentiality (at rest)	FIREWORKS databases are encrypted using a unique encryption key for each customer, which are managed by bioMérieux.
Health Data Transmission Confidentiality (in transit)	FIREWORKS data are encrypted in transit using TLS v1.2 or greater.
Health Data Transmission Integrity	Data sent from BIOFIRE® Systems will be re-sent if a communication interruption occurs.
Health Data De-Identification	Health data stored in FIREWORKS are encrypted. bioMérieux employees do not have access to health data.
Data Backup and Disaster Recovery	FIREWORKS utilizes the data backup and disaster recovery policies provided by AWS.
Health Data Integrity and Authenticity	FIREWORKS includes integrity monitoring features that alert of potential failures that could affect data integrity.
Encryption Key Management	bioMérieux manages the encryption keys for each customer with defined policies surrounding access by AWS services.
DDOS Protection	FIREWORKS has DDOS protection provided by AWS.
Malware Detection/Protection	N/A - Please refer to System-specific documentation for more details.
Configuration of Security Features	FIREWORKS allows admin users to modify institution locations and user management.
Patch Management	FIREWORKS automatically updates the software as new security/enhancement patches are released.
Third-Party Components in Product Lifecycle Roadmaps	bioMérieux works with our third-party cybersecurity partners to perform risk assessments of FIREWORKS.

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

PIONEERING DIAGNOSTICS