BIOMÉRIEUX

CLARION™
CYBERSECURITY

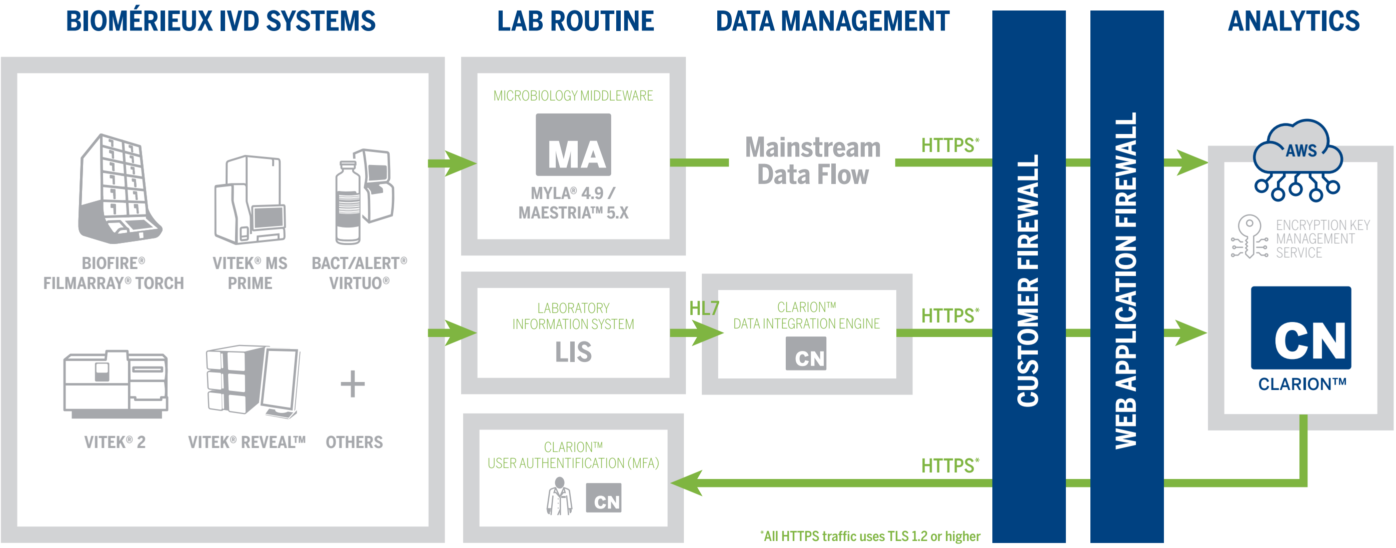
CN
CLARION™

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 by Design.



BIOMÉRIEUX IVD SYSTEMS

BIOFIRE® FILMARRAY® TORCH

VITEK® MS PRIME

BACT/ALERT® VIRTUO®

VITEK® 2

VITEK® REVEAL™

+ OTHERS

LAB ROUTINE

MICROBIOLOGY MIDDLEWARE

MA

MYLA® 4.9 / MAESTRIA™ 5.X

LABORATORY INFORMATION SYSTEM

LIS

CLARION™ USER AUTHENTIFICATION (MFA)

CN

DATA MANAGEMENT

Mainstream Data Flow

HL7

CLARION™ DATA INTEGRATION ENGINE

CN

HTTPS*

HTTPS*

HTTPS*

CUSTOMER FIREWALL

WEB APPLICATION FIREWALL

ANALYTICS

AWS

ENCRYPTION KEY MANAGEMENT SERVICE

CN

CLARION™

*All HTTPS traffic uses TLS 1.2 or higher

SURVEILLANCE

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

- For every new CLARION™ 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

CYBERSECURITY RISK ANALYSIS

- As for product safety, a cybersecurity risk analysis is performed on each CLARION™ release.

- This cybersecurity risk analysis and cybersecurity state-of-the-art good practices are an input to CLARION™ developments and architecture design.

PROACTIVITY

SUPPORT BY SECURITY EXPERTS

- CLARION™ 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 CLARION™ release.

BIOMÉRIEUX

	CLARION™ FEATURES
Automatic logoff	The system automatically logs off users based on a period of inactivity.
Audit Controls	CLARION™ allows to collect + track usage metrics, collect, centralized & monitor log files, and set alarms.
Authorization	User authorization ensures that each and every user possesses the appropriate permissions before allowing access to CLARION™
Cybersecurity Product Update	bioMérieux maintains monthly post market monitoring of potential vulnerabilities. All vulnerabilities are assessed impact/likelihood and corrected in a patch if relevant.
Health Data De-identification	Health data are encrypted for backups and for support purposes. Data that are extracted for support purposes are de-identified.
Data Backup and Disaster Recovery	bioMérieux has selected AWS as the cloud service provider due to the comprehensive disaster recovery services. A code repository tool maintains an application image for application recovery purposes.
Health Data Integrity & Authenticity	The system includes integrity monitoring features that alert on potential failures that could affect data integrity, including database referential integrity to prevent data corruption.
Malware Detection/Protection	CLARION™ systematically deploys TrendMicro for antivirus analysis and malware detection.
Node Authentication	CLARION™ securely communicates with other network elements cf. industry standard best practice.
Person Authentication	CLARION™ utilizes and enforces Multi-Factor Authentication (MFA). CLARION™ supports industry standard third-party applications, which include but are not limited to, Microsoft Authenticator and Google Authenticator. CLARION™ supports SMS based MFA.
Third-party Components in Product Lifecycle Roadmaps	bioMérieux monitors CLARION™ components for emerging vulnerabilities and issues product updates as needed. CLARION™ utilizes AWS tools & services to deliver a seamless, secure end-user experience.
System and Application Hardening	bioMérieux conducts independent third-party testing (incl. penetration testing & vulnerability scanning).
Security Guides	bioMérieux publishes technical and architectural guidance for secure deployment and configuration.
Encryption Key Management	The use of KMS (Key Management Service) in AWS enables secure and centralized key management for data encryption and access control.
Transmission Confidentiality	The system supports HTTPS with TLS 1.2 or higher encryption.
Transmission Integrity	The system is able to detect and recover from communication failures for critical messaging.
AWS Security Standards & Compliance Certifications	AWS supports 143 security standards and compliance certifications, including HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-1714. These standards and certifications The system is able to detect and recover from communication failures for critical messaging.

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