

CLARION™ CYBERSECURITY



CLARION™

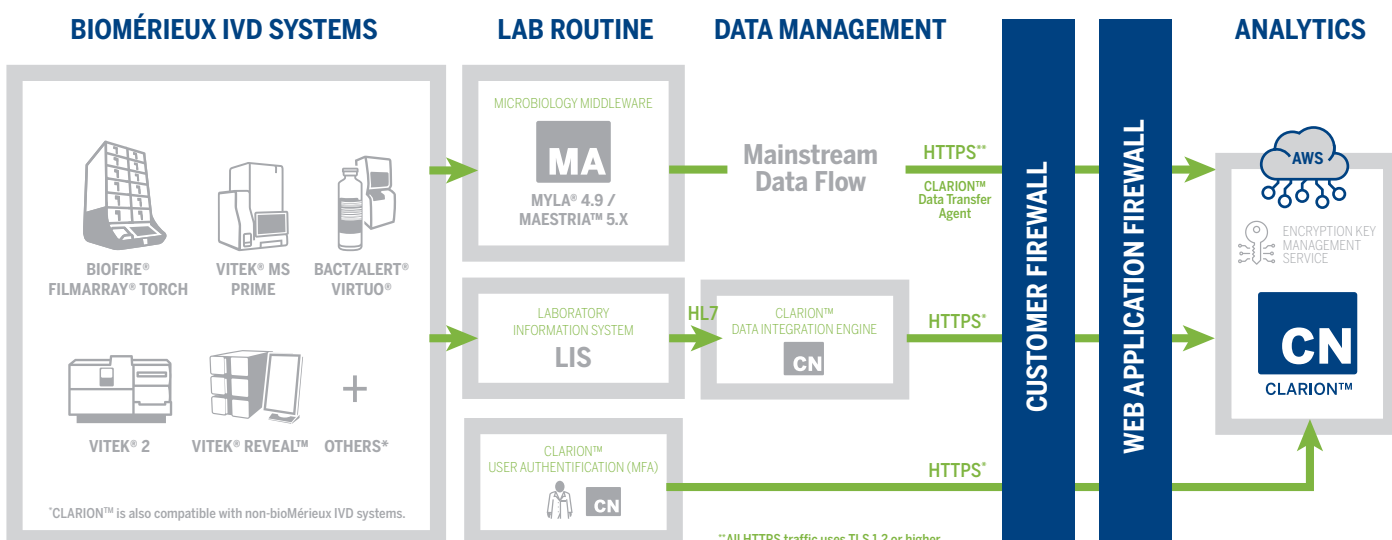


CYBER SECURITY

**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 security.officer@biomerieux.com





SECURE BY DESIGN

Threat modelling

Analysis using a structured representation of all the information that affects the security of CLARION™.

Risk analysis

For product safety, a cybersecurity risk analysis is conducted with each CLARION™ release. This cybersecurity risk analysis and cybersecurity best practices are input into CLARION™ developments and architectural design.

VULNERABILITY SURVEILLANCE

Vulnerability check

External cybersecurity experts are involved all along our development projects, and scans performed based on Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE) reports. An overview is exposed to our experts to identify and track system and network vulnerabilities to evaluate the overall security of the integrated solution.

Threat monitoring

CLARION™ leverages state-of-the-art threat monitoring services provided by Amazon Web Services (AWS) and the bioMérieux Security Operations Center (SOC).

SAFE IMPLEMENTATION

Standard-based development

Our secure development processes follow industry standard best practices and guidelines as outlined within the Secure Software Development Framework (NIST SP 800-218.)



SECURITY FEATURES	CLARION™ FEATURES
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 Encryption	Health data are encrypted for backups and for support purposes.
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.
User 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. bioMérieux will work with the customer to ensure the on-prem components are installed and configured in a secure manner during the implementation process.
Encryption Key Management	The use of KMS (Key Management Service) in AWS enables secure and centralized key management for data encryption and access control. Health Data are encrypted for backups and for support purposes.
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 800-171.

Data Privacy And Data Security Laws And Regulations

bioMérieux is a trusted partner to thousands of healthcare entities in connection with the protection of the confidentiality, privacy, and security of patient health information. As a global company, bioMérieux has extensive experience in navigating the increasingly complex and ever-evolving landscape of relevant data privacy and data security regulations globally. These regulations not only include HIPAA in the US and the GDPR in the EU, but also other applicable national, regional, and local data privacy and data security laws and regulations. To promote compliance with applicable data privacy and data security laws and regulations, bioMérieux has long-standing programs overseen by experienced data privacy and cybersecurity teams. Such programs include the implementation of industry standard security reviews, assessments and audits intended to ensure that the development of bioMérieux software solutions, and including any third-party components, meet applicable data privacy and data security laws and regulations.

08-25 / BMX.1158165 / 9328112.002/GB/B Document and/or picture not legally binding. Modifications by bioMérieux can be made without prior notice / BIOMÉRIEUX, the BIOMÉRIEUX logo, PIONEERING DIAGNOSTICS, BACT/ALERT, BIOFIRE, CLARION, FILMARRAY, MAESTRIA, MYLA, REVEAL, VIRTUO and VITEK are used, pending and/or registered trademarks belonging to bioMérieux, or one of its subsidiaries, or one of its companies. / Any other name or trademark is the property of its respective owner. / bioMérieux S.A. RCS Lyon 673 620 399

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