BIOMÉRIEUX

EMAG® / NUCLISENTRAL®

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 by Design.

SURVEILLANCE

EVERY WEEK

- The EMAG®/NUCLISENTRAL® platform is scanned for cybersecurity threats using an external reference tool.
- All vulnerabilities are assessed (impact/criticality) and corrected in a patch if relevant.

EVERY MONTH

- A cybersecurity bulletin is issued internally.

EVERY RELEASE

- For every new EMAG® /NUCLISENTRAL® release & platform, penetration tests are performed by external companies.
- Each EMAG® /NUCLISENTRAL® release integrates cybersecurity updates.

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

SUPPORT BY SECURITY EXPERTS

- As for product safety, a cybersecurity risk analysis is performed on each EMAG®/NUCLISENTRAL® release.
- This cybersecurity risk analysis and cybersecurity state-of-the-art good practices are an input to EMAG®/NUCLISENTRAL® developments and architecture design.

BIOMÉRIEUX

REQUIREMENTS	EMAG® CONNECTION THROUGH NUCLISENTRAL®
Automatic logoff	Configurable period of inactivity before logoff
Audit Controls	Centralization of laboratory workflow and user data events in an audit log
Authorization	Role-based access control
Configuration of security features	Authorized users can configure system functionalities
Cyber security product upgrades	Monthly post market monitoring
Health Data De-identification	Health data are encrypted for backups and for support purposes
Data Backup and Disaster Recovery	Authorized users can automate backups. The system can be restored to a prior date with the assistance of bioMérieux support.
Health Data Integrity and Authenticity	Monitoring features, alert on potential failures that could affect data integrity.
Malware Detection/Protection	Robust Secure Development Lifecycle. Microsoft Windows Defender antivirus software is installed by default on the system. The customer can also install the anti-virus of his choice and apply his own security policy.
Node Authentication	EMAG® supports communication authentications and integrates an internal firewall.
Person Authentication	Configurable password authentication for users, that can be linked with a Windows centralized authentication provider. The web login interface of EMAG® system may be integrated on the customer authentication service.
Physical Locks on Device	Does not meet
Third-party Components in Product Lifecycle Roadmaps	Monitor components for emerging vulnerabilities and issue product updates
System and Application Hardening	Independent third party testing of the device OS and network settings
Security Guides	bioMérieux publishes technical and architectural guidance for the secure deployment and configuration of devices, include security whitepaper, MDS2, and SBoM.
Health Data Storage Confidentiality	Encryption of backups
Transmission Confidentiality	EMAG® supports Transport Layer Security (TLS)
Transmission Integrity	Detect and recover from communication failures for critical messaging
Other	Windows 10 Enterprise LTSC or LTSB 2019

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

PIONEERING DIAGNOSTICS