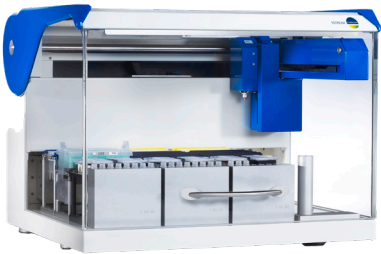


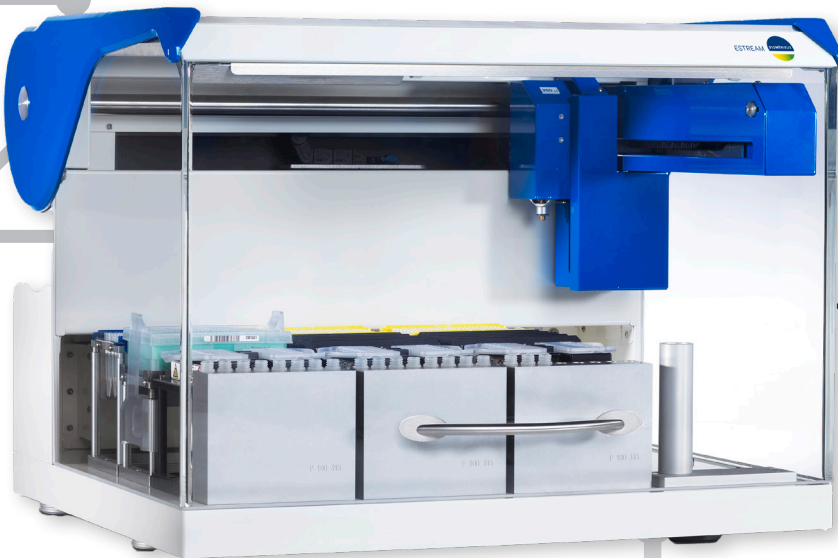
ESTREAM[®] CYBERSECURITY



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

- ESTREAM® platform is being scanned for cyber security 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 ESTREAM® release, penetration tests are performed by external companies
- Each ESTREAM® 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 ESTREAM® release
- This cybersecurity risk analysis and cybersecurity state-of-the-art good practices are an input to ESTREAM® developments and architecture design architecture design.

REQUIREMENTS	ESTREAM®
Automatic logoff	The system automatically logs off users based on a configurable period of inactivity
Audit Controls	ESTREAM® General Laboratory Use capture user events, data events and remote service activity in an audit trail.
Authorization	ESTREAM® leverages Windows user rights management which enables role-based access control ESTREAM® application is designed to run in non-administrative operating system accounts to prevent tampering.
Configuration of security features	ESTREAM® system enables authorized users to configure users to have access to various system functionalities such as audit trail and user management.
Cyber security product upgrades	Monthly postmarket monitoring and patching of potential vulnerabilities
Data Backup and Disaster Recovery	ESTREAM system enables authorized users to automate backups and retention settings, as well as configuring data backups in an encrypted format and stored on a local network or server. The system can be restored to a prior date with the assistance of bioMérieux support.
Malware Detection/Protection	Microsoft Windows Defender anti-virus 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	ESTREAM® leverages Windows to enable configurable password authentication.
Person Authentication	The service providing authentication to the system can be configured according to the security policy of the customer company and associated with a Windows centralized authentication provider. The web login interface of ESTREAM® system may be integrated on the customer authentication service.
Third-party Components in Product Lifecycle Roadmaps	Monitor components for emerging vulnerabilities and issue product updates
System and Application Hardening	bioMérieux conducts independent third-party testing of the device operating system and network settings, including active ports and services
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	The system enables encryption of backups.
Transmission Confidentiality	Not applicable (by ARGENE® CONNECT : the system supports HTTPS with TLS 1.2 encryption).
Transmission Integrity	Not applicable (by ARGENE® CONNECT : the system is able to detect and recover from communication failures for critical messaging)
Other	Windows 10 Enterprise LTSC or LTSC 2019



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.

9323581 002/GB/A/ Document and/or picture not legally binding. Modifications by bioMérieux can be made without prior notice / BIOMÉRIEUX, the BIOMÉRIEUX logo, PIONEERING DIAGNOSTICS and ESTREAM 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 / Printed in France

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