BIOMÉRIEUX

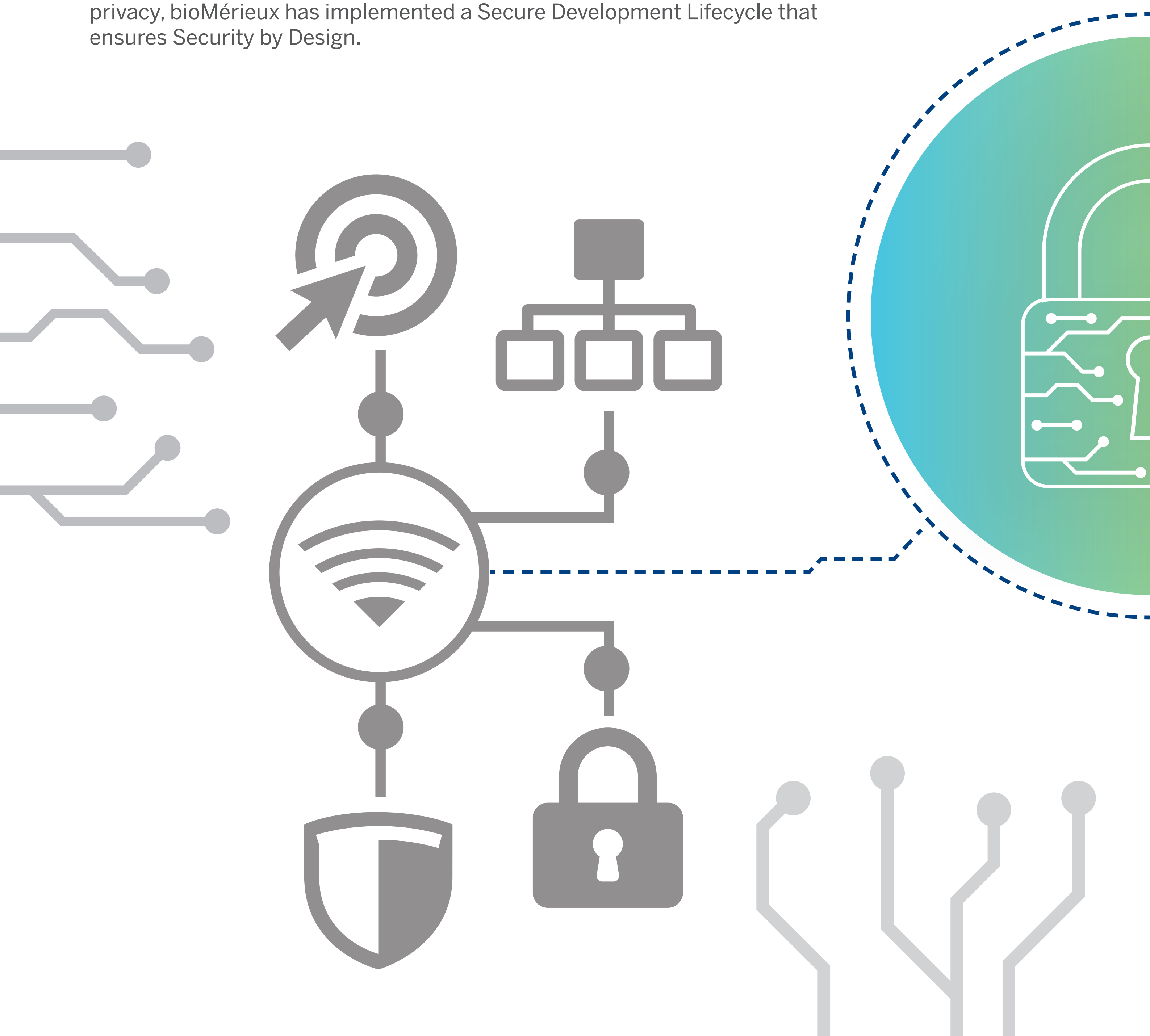
VILINK®
CYBERSECURITY

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

CONTINUOUSLY

- Information coming from different security sources, including CERTs, are made available daily to the bioMérieux cybersecurity team.

EVERY MONTH

- VILINK platform is scanned for cybersecurity vulnerabilities using an external reference tool.
- All new vulnerabilities reported by the security monitoring activity are reviewed monthly.
- Vulnerabilities are assessed for severity, technical response, and implementation complexity to establish a response plan.

EVERY RELEASE

- Prior to each major release, VILINK® undergoes Risk Analysis, Vulnerability Assessment and Penetration Test, and Vulnerability Scans.
- Each VILINK release integrates cybersecurity updates.

EXPERTISE

SUPPORT BY SECURITY EXPERTS

- Dedicated internal cybersecurity team, reinforced by recognized expertize consultants (Healthcare, Department of Defense, Space industry) to maintain state of the art security features.

PROACTIVITY

SUPPORT BY SECURITY EXPERTS

We follow the following standards for each software release:

- AAMI TIR57:2016, CLSI AUTO 9, 21CFR11
- Cybersecurity state-of-the-art good practices for VILINK coding and architecture design (cybersecurity by design, code revue, threat models)
- Data privacy assesment : GDPR, HIPAA

BIOMÉRIEUX

ISO 80001 REQUIREMENTS	VILINK® FEATURES
Person Authentication	All VILINK® user accounts and authorizations are controlled by a bioMérieux Identity and Access Management. VILINK® authentication is configured according to bioMérieux security policy including Multi Factor Authentication, and associated with Azure Active Directory SSO.
Authorization	Customer must acknowledge the remote access request before a bioMérieux user can connect to the bioMérieux system in the lab.
Automatic Logoff	The system automatically logs off users, based on a period of inactivity following cybersecurity best practices.
Audit Controls	Audit trails are available to VILINK® administrator account for 1 year. It contains information related to the VILINK® connection session and actions performed.
Health Data Storage Confidentiality	VILINK® does not collect Health data by default, nor store it. In case of investigation, after customer acceptance, a data backup can be collected and stored for a limited time in a secure controled space.
Health Data Transmission Confidentiality	The communication between the VILINK® Agent and the VILINK® Server support HTTPS with TLS 1.2 encryption (VILINK® Agent) and TLS 1.3 (Web browser) through a 256 bits encryption key.
Health DataTransmission Integrity	De-identification is managed by the analytical system.
Health Data De-Identification	VILINK® is based on a High Availability infrastructure through Microsoft Azure services, and supported by a Disaster Recovery Plan.
Encryption Key Management	Encryption key are managed a trusted third party.
Data deletion (GDPR)	VILINK® does not collect Health data by default, nor stores it.
Malware Detection/Protection	VILINK® applies Cloud security good practices and implements Defender for Cloud (Azure).
Configuration of Security Features	VILINK® applies Cloud security good practices.
Patch Management	bioMerieux maintains a monthly postmarket monitoring and patching of potential vulnerabiltes.
Training	VILINK® users follow a VILINK® training to be VILINK® certified.
Third-party Components in Product Lifecycle Roadmaps	bioMérieux maintains regular monitoring of third party components through its cybersecurity postmarket process.
Security Guides	bioMérieux publishes technical and architectural guidance for the secure deployment and configuration of devices, including security whitepaper.
Cybersecurity Product Upgrades	bioMérieux maintains a monthly postmarket monitoring and patching of potential vulnerabiltes.
System and Application Hardening	bioMérieux conducts independent third party testing, including penetration tests, of the device operating system and network settings, including active ports and services.

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