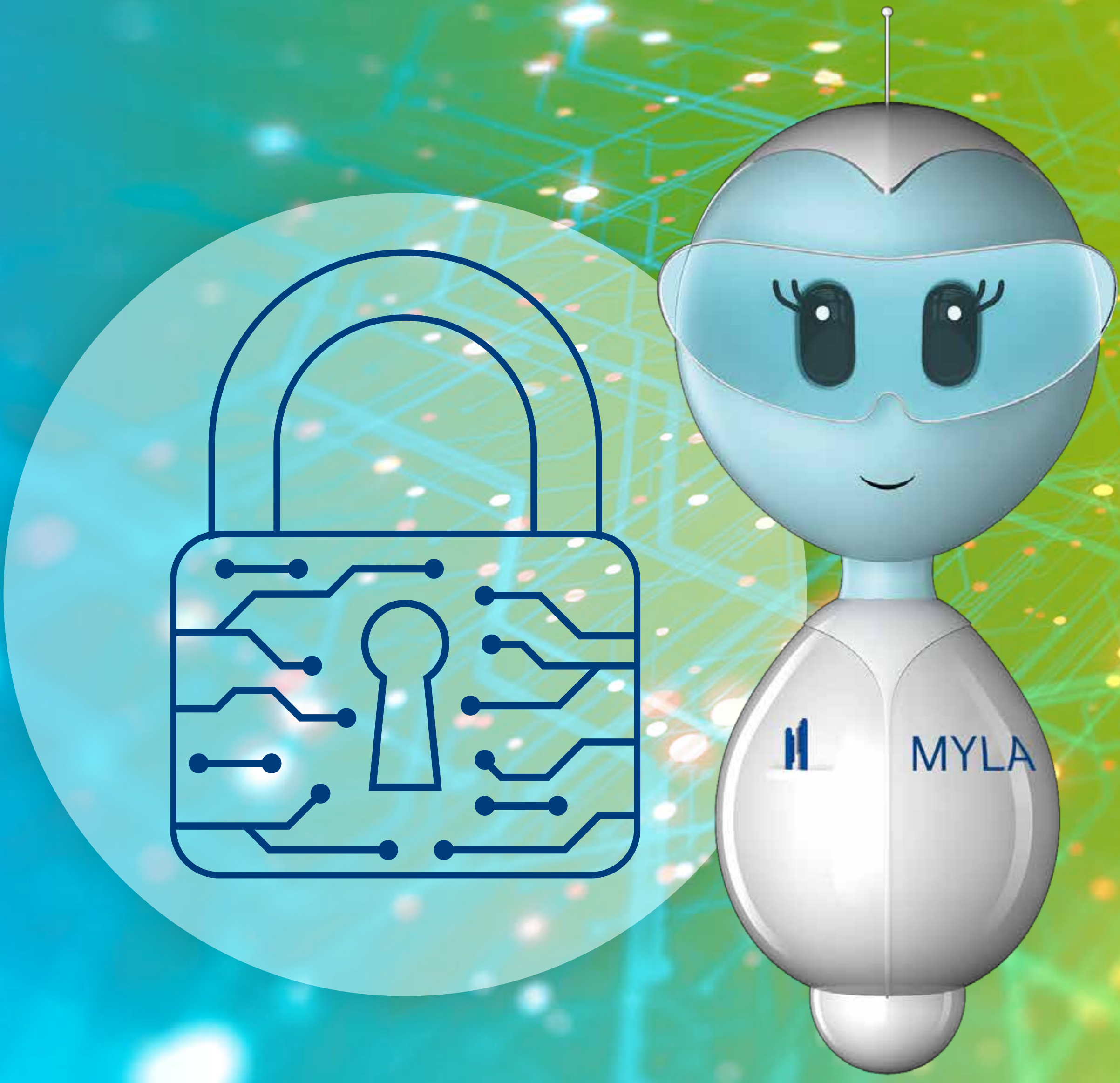
MYLA®

Cybersecurity by Design



Your Ally in Advancing Quality

PIONEERING DIAGNOSTICS

CYBER SECURITY BY DESIGN

Cybersecurity is integrated in the design of our products. Supported by our partners and bioMérieux experts in cybersecurity and data privacy, bioMérieux has implemented a Secure Development Lifecycle that ensures Security by Design and follow the highest cybersecurity standard ISO/IEC 27002.

SURVEILLANCE

Every Week

- MYLA® 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 MYLA® release & platform, penetration tests are performed by external companies
- Each MYLA® release integrates cybersecurity updates

PROACTIVITY

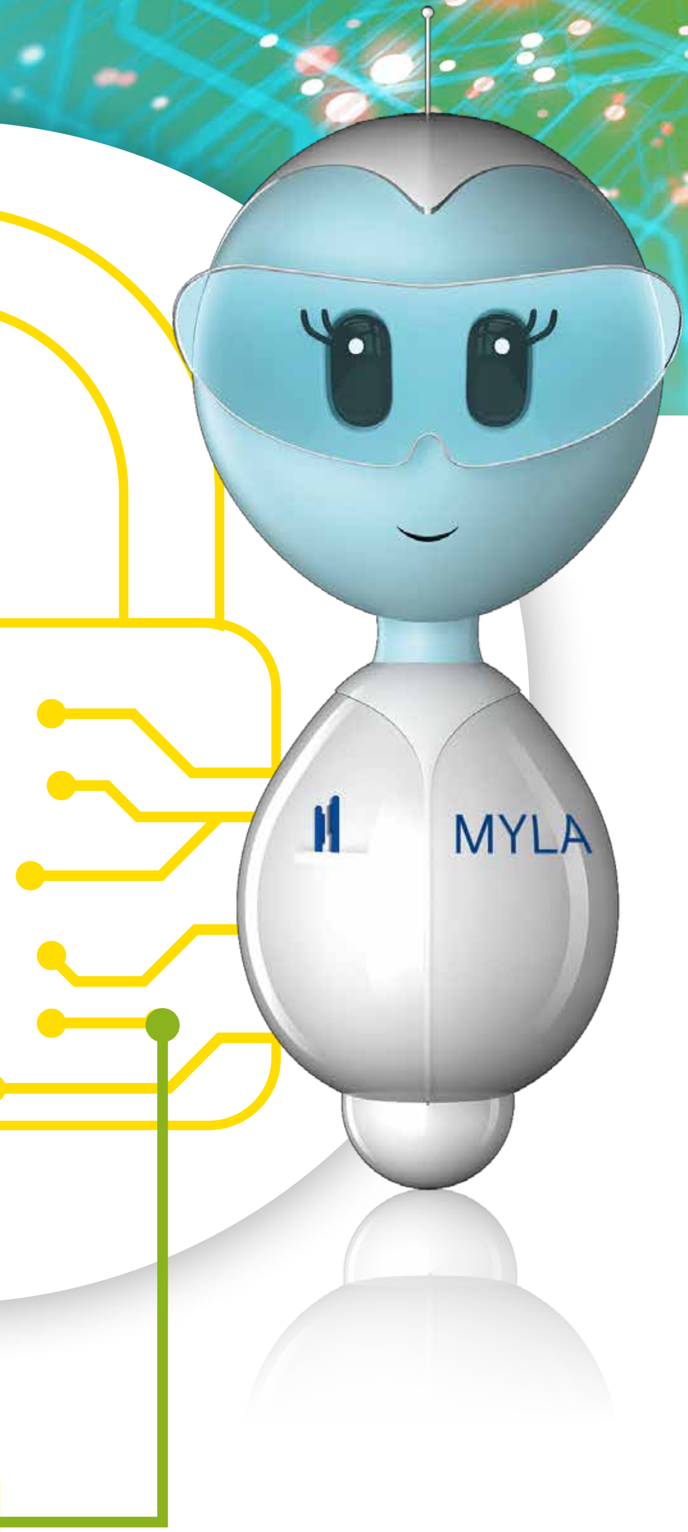
Cybersecurity Risk Analysis

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

SECURITY

Support by Security Experts

- MYLA® is developed by an experienced and skilled IT staff using a proven coding methodology in the development of sensitive platforms for pharmaceeutical companies to ensure data security.



Requirements	MYLA®
Automatic logoff	✓
Audit Controls	✓
Authorization	✓
Configuration of security features	✓
Cyber security product upgrades	✓
Data De-identification	✓
Data Backup and Disaster Recovery	✓
Data Integrity and Authenticity	✓
Malware Detection/Protection	✓
Node Authentication	✓
Person Authentication	✓
System and Application Hardening	✓
Security Guides	✓
Data Storage Confidentiality	✓
Transmission Confidentiality	✓
Transmission Integrity	✓

How does MYLA® ensure Compliance with the Highest International Standard (ISO/IEC 27002)?

	MYLA®
Proactivity:	
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
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.
Surveillance:	
Malware Detection/Protection	Robust Secure Development Lifecycle. 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.
Cyber security product upgrades	Third party components in product lifecycle roadmaps.
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.
Security:	
Transmission Integrity	Detect and recover from communication failures for critical messaging
Transmission Confidentiality	HTTPS with TLS 1.2 encryption
Node Authentication	MYLA® 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 MYLA® system may be integrated on the customer authentication service.
Data De-identification	Data are de-identified or encrypted for backups and for support purposes
Data Integrity and Authenticity	Monitoring features, alert on potential failures that could affect data integrity
Health Data Storage Confidentiality	Encryption of backups
Other	Windows 10 ENTERPRISE LTSC or LTSB 2019 for the MYLA® PC or Windows Server 2016 & 2019 for the Virtual Machine. 21 CFR part 11 compliance.