BIOMÉRIEUX

ENDONEXT™ Software

Cybersecurity by design

Your Ally in Advancing Quality

PIONEERING DIAGNOSTICS

CYBERSECURITY BY DESIGN

ENDONEXT™ software is designed to ensure the security and accuracy of data in quantitative endotoxin testing. It helps ensuring data integrity, meeting the stringent requirements of regulatory agencies. Specifically, it complies with 21 CFR Part 11 and global data integrity guidelines, ensuring that your results are both trustworthy and secure.

SURVEILLANCE

- ENDONEXT™ platform is scanned for cybersecurity vulnerabilities using an external reference tool. All vulnerabilities are assessed.
- A cybersecurity bulletin is issued monthly.

EXPERTISE

- Either at rest or in transit, bioMérieux enforces data protection by implementing security features in compliance with current standards, such as cryptographic measures, role-based access control, or a strong backup and restore process.
- Using PostgreSQL database, confidentiality, integrity, availability and authenticity of all data processed by ENDONEXT™ is ensured during its whole lifecycle.
- For every new ENDONEXT™ software release, penetration tests are performed by external companies to detect new vulnerabilites.
- All vulnerabilities are assessed via risk assesment and corrected in a patch or next version if required.

PROACTIVITY

- Development and maintenance of ENDONEXT™ software are perfomed following a secure development lifecycle integrating mandatory security activities and in compliance with standards and guidelines such as 21 CFR 11.
- A cybersecurity risk assessment is perfomed prior to each ENDONEXT™ release to ensure safety, security, and privacy.

How does ENDONEXT™ ensure compliance with the Highest International Standards?

Benefits	Requirements	ENDONEXT™ Features
Authentication & Authorization	Automatic logoff	The ENDONEXT™ software forces automatic logoff after a customizable period of inactivity.
	Authorization	ENDONEXT™ leverages Windows user rights management and build-in Software Accounts Authorization, which enables role-based access control. ENDONEXT™ applications are designed to run in non-administrative operating system accounts to prevent tampering.
	Person Authentication	ENDONEXT™ manages people authentication via integrated account management or via LDAP/LDAPS.
	Configuration of Security Features	The software authentication service can be configured (based on three levels) according to the security policy of the customer.
	Node Authentication	ENDONEXT™ implements authentication using JWT tokens.
Availability	Network Controls	ENDONEXT™ does not implements network controls. As it is deployed in the customer's environment, the firewall is configured by the customer.
	Malware Detection/ Protection	The customer can also install their coporate anti-malware solution, and apply their own security policy.
Data	Classification(s) of Data Stored	ENDONEXT™ doesn't store or processes any sensitive data, but it could potentially store personal data like usernames.
	Data Backup and Disaster Recovery	ENDONEXT™ system enables authorized users to automate backups settings, as well as configuring data backups in an encrypted format and stored on a local drive (prerequisites applicable). The system can be restored to a prior date with the assistance of bioMérieux support.
	Transmission Confidentiality	Data is encrypted using https during transmission. TLS 1.2 is supported.
	Transmission Integrity	Enabling TLS 1.2 for communications grants native transmission integrity by protocol design.
Audit	Audit Controls	Audit Trail records cannot be deleted, are stamped, filtered and can be exported.
	Regulatory Compliance	ENDONEXT™ software is designed to comply with 21 CFR11.
Maintenance	System and Application Hardening	Cybersecurity risk assessments, penetration testing, SAST (static application security testing), SCA (software composition analysis), and manual code review are performed and vulnerabilities are remediated (if required) as part of the secure SDLC (software development lifecycle) to ensure the application is hardened appropriately.
	Cybersecurity product updates	ENDONEXT™ will receive periodic updates as needed to remediate discovered vulnerabilities.
	Third-party Components in Product Lifecycle Roadmaps	Software Composition Analysis is performed to facilitate SBOM generation and to identify libraries and third-party components utilized to ensure all components and libraries stay up to date.
Other	Security Guides	A detailed Product Security Technical Whitepaper will be available for ENDONEXT™.
	Scope	This assesment is applicable for ENDONEXT™ software version 3.

bioMérieux S.A. • 69280 Marcy l'Étoile • France • Tel.: + 33 (0)4 78 87 20 00 • Fax: +33 (0)4 78 87 20 90
www.biomerieux.com