BIOMÉRIEUX

VITEK®

Cybersecurity by design

Your Ally in Advancing Quality

PIONEERING DIAGNOSTICS

CYBERSECURITY BY DESIGN

PROACTIVITY

- Development and maintenance of the VITEK® COMPACT PRO software is performed following a secure development lifecycle integrating mandatory security activities and in compliance with standards and guidelines such as OWASP, IEC 62304, TIR57, 21CFR11, CLSI AUTO9 and CLSI AUTO11.
- A cybersecurity risk assessment is performed prior to each VITEK® COMPACT PRO release to ensure safety, security, and privacy.

SURVEILLANCE

- Defense-in-depth principles have been applied for securing VITEK® COMPACT PRO by implementing state-of-the-art development methods to provide maximum reliability.
- The VITEK® COMPACT PRO platform is scanned for cybersecurity threats using an external reference tool. All vulnerabilities are assessed (impact/criticality)
- A cybersecurity bulletin is issued internally.

VITEK® COMPACT PRO is an automated system that performs organism identification and antimicrobial susceptibility testing in human and veterinarian applications; as well as organism identification testing in industrial applications for environmental monitoring and quality control. The software version for this system is VITEK® V10.0.

EXPERTISE

- Whether 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, malware protection, and a strong backup and restore process.
- For every new VITEK® COMPACT PRO software release, penetration tests are performed by external companies to detect new vulnerabilities and threats. All vulnerabilities are assessed (impact/criticality) and corrected if necessary

How does VITEK® COMPACT PRO ensure Compliance with the Highest International Standards?

Benefits	Requirements	VITEK® V10.0 SOFTWARE Features
Authentication & Authorization	Automatic logoff	The VITEK® V10.0 software forces automatic log off after a configurable period of inactivity.
	Authorization	The VITEK® V10.0 software supports Role Base Access Control (RBAC) by leveraging built-in Software account authorization and authentication.
	Account Authentication	VITEK® COMPACT PRO manages account authentication through the local machine Windows password policy and/or a Windows centralized authentication provider.
	Configuration of Security Features	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 the VITEK® COMPACT PRO system may be integrated into the customer's authentication service.
	Node Authentication	VITEK® COMPACT PRO implements mutual authentication through certificates between modules.
Availability	Network Controls	VITEK® COMPACT PRO implements network controls through Windows Firewall configuration, restricting traffic only to specific ports and services.
	Malware Detection/ Protection	Microsoft Windows Defender anti-virus software is installed by default on the system. Customers can also install their corporate anti-malware solution, and apply their own security policy.
	Web Browser Compatibility	The browser to web server communication is secured by forcing https. Supported browsers: Edge, Chrome and Firefox.
Data	Classification(s) of Data Stored	VITEK® COMPACT PRO stores and processes PII and PHI.
	Health Data De-Identification	Local hard drives, databases or files containing PHI/PII are never to be removed from the customer's site without written authorization from the customer.
	Health Data Storage Confidentiality	Local hard drives are encrypted at disk level using Windows BitLocker.
	Health Data Integrity and Authenticity	The system includes integrity monitoring features that alert on potential failures that could affect data integrity, including database referential integrity to prevent data corruption.
	Data Backup and Disaster Recovery	The VITEK® COMPACT PRO system enables authorized users to automate backups and retention settings, as well as configure the location of the backup, such as an internal hard drive, USB storage, or network storage. The system can be restored to a prior date with the assistance of bioMérieux support.
	Transmission Confidentiality	Data is encrypted using AES 256 prior to transmission. TLS 1.2 an TLS 1.3 are supported.
	Transmission Integrity	The use of TLS 1.2/1.3 for communications grants native transmission integrity by protocol design.
	Encryption Key Management	BitLocker encryption key is managed by the TPM chip.
Audit	Audit Controls	Audit Trail records cannot be deleted, are time-stamped and can be exported.
	Regulatory Compliance	A Data Privacy Impact Assessment and HIPAA assessment have been performed by a third party to confirm GDPR and HIPAA compliance.
Maintenance	System and Application Hardening	Cybersecurity risk assessments, penetration testing, static application security testing, vulnerability monitoring, and manual code review are performed, and vulnerabilities appropriately remediated as part of the secure SDLC to ensure the system and application are hardened appropriately and the OS is hardened accordding to Windows 10 STIG V2 standard.
	Cybersecurity product updates	VITEK® COMPACT PRO will receive updates as needed to remediate uncontrolled security risk.
	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 by the solution to ensure all components and libraries stay up to date.
Other	Security Guides	A detailed Product Security Technical Whitepaper is available for VITEK® COMPACT PRO.
	Others	This assesment is applicable for other legacy systems under the VITEK® 2 software version 10: • VITEK® 2 • VITEK® 2 COMPACT • VITEK® 2 XL

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