Product Security White Paper

BD Rhapsody™ Scanner (RUO) with BD Rhapsody™ Scanner Software v2.0

BD is committed to providing secure products to our customers given the important benefits they contribute to science. We value the confidentiality, integrity and availability of all information, including protected health and personally identifiable information (e.g., PHI, PII, and other types of personal data and sensitive data) and are committed to comply with applicable regional, federal and local privacy and security laws and regulations, including the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) (EU) 2016/679.

BD has implemented reasonable administrative, technical and physical safeguards to help protect against security incidents and privacy breaches involving a BD product, provided those products are used in accordance with BD instructions for use. However, as systems and threats evolve, no system can be protected against all vulnerabilities, and we consider our customers the most important partner in maintaining security and privacy safeguards. If you have any concerns, we ask that you bring them to our attention, and we will investigate. Where appropriate, we will address the issue with product changes, technical bulletins and/or responsible disclosures to customers and regulators. BD continuously strives to improve security and privacy throughout the product lifecycle using practices such as:

- Privacy and Security by Design
- Product and Supplier Risk Assessment
- Vulnerability and Patch Management
- Secure Coding Practices and Analysis
- Vulnerability Scanning and Third-Party Testing
- Access Controls appropriate to Customer Data
- Incident Response
- Clear paths for two-way communication between customers and BD

If you would like to report a potential product related privacy or security issue (incident, breach or vulnerability), please contact the BD Product Security team:

Site: http://www.bd.com/productsecurity/
Email: ProductSecurity@bd.com

Mail:

Becton, Dickinson and Company
Attn: Product Security
1 Becton Drive
Franklin Lakes, New Jersey 07417-1880

The purpose of this document is to detail how our security and privacy practices have been applied to the BD Rhapsody™ Scanner v2.0, what you should know about maintaining security of this product and how we can partner with you to ensure security throughout this product's lifecycle.

Contents

Product Description

The BD Rhapsody™ Scanner is an automated scanner designed to image BD Rhapsody™ Cartridges for the purpose of determining the number of cells loaded in the cartridge that are paired with a single barcoded bead. The BD Rhapsody™ Scanner consists of an embedded PC running Microsoft™ Windows™ 10, an integrated 21" touchscreen display, and hardware to support the intended imaging. There is one USB v3 port on the side of the instrument intended for customer use (data transfer). The rear of the instrument contains two USB v2 ports and one Gigabit Ethernet port.

Hardware Specifications

- Advantech™ AIMB-275 Motherboard
- Processor: Intel™ Core i7-6700 CPU @ 3.40 GHz
- RAM: 16 GB
- Display: FEMA P/N GM12801024A-190-TTX1NLW-HTGFF

Operating Systems

- Microsoft™ Windows™ 10 Enterprise 2015 LTSB 64-bit

Third-Party Software

Vendor and Name	Version	Description
FAULHABER USBX Adapter (Driver Removal)	N/A	USB driver support
Intel™ Processor Graphics	21.20.16.4534	Graphics chipset driver
Microsoft™ Visual C++ 2013 Redistributable (x64)	12.0.30501	Visual Studio redistributable library

Vendor and Name	Version	Description
Microsoft™ Visual C++ 2013 Redistributable (x86)	12.0.30501	Visual Studio redistributable library
Microsoft™ Visual C++ 2013 x86 Additional Runtime	12.0.21005	Visual Studio redistributable library
Microsoft™ Visual C++ 2013 x86 Minimum Runtime	12.0.21005	Visual Studio redistributable library
Microsoft™ Visual C++ 2015 Redistributable (x86)	14.0.24215	Visual Studio redistributable library
Microsoft™ Visual C++ 2015 x86 Additional Runtime	14.0.24215	Visual Studio redistributable library
Microsoft™ Visual C++ 2015 x86 Minimum Runtime	14.0.24215	Visual Studio redistributable library
Microsoft™ Visual C++ 2015-2022 Redistributable (x64)	14.30.30704	Visual Studio redistributable library
Basler™ Pylon Miscellaneous Documents x86	5.0.12.11830	Digital camera development libraries
Basler™ Pylon PreventOldInstallerFromInstallation	5.0.12.11830	Digital camera development libraries
Basler™ Pylon .NET Runtime Environment x86	5.0.12.11830	Digital camera development libraries
Basler™ Pylon 5 Camera Software Suite	5.0.12.11830	Digital camera development libraries
Basler™ Pylon Camera Software Suite product info	5.0.12.11830	Digital camera development libraries
Basler™ Pylon RemoveLegacyModules	5.0.12.11830	Digital camera development libraries
BD Rhapsody™ HT Xpress System Prerequisite	2.0.0.0	BD component library
Tera Term 4	4.101	Terminal program for serial communications
USB Camera Driver	4.3.0	Digital camera development libraries
USB COM Installer	6.3.2	USB Serial communications driver

Network Ports and Services

The BD Rhapsody™ Scanner has an Ethernet connector on the rear panel for product development and testing purposes only. The network interface is not configured for network security and the Scanner device should not be connected to the customer network.

Sensitive Data Transmitted

BD Rhapsody™ Scanner does not transmit instrument data. Instrument data is stored on the device in text files and .png images. Data files are not encrypted.

Sensitive Data Stored

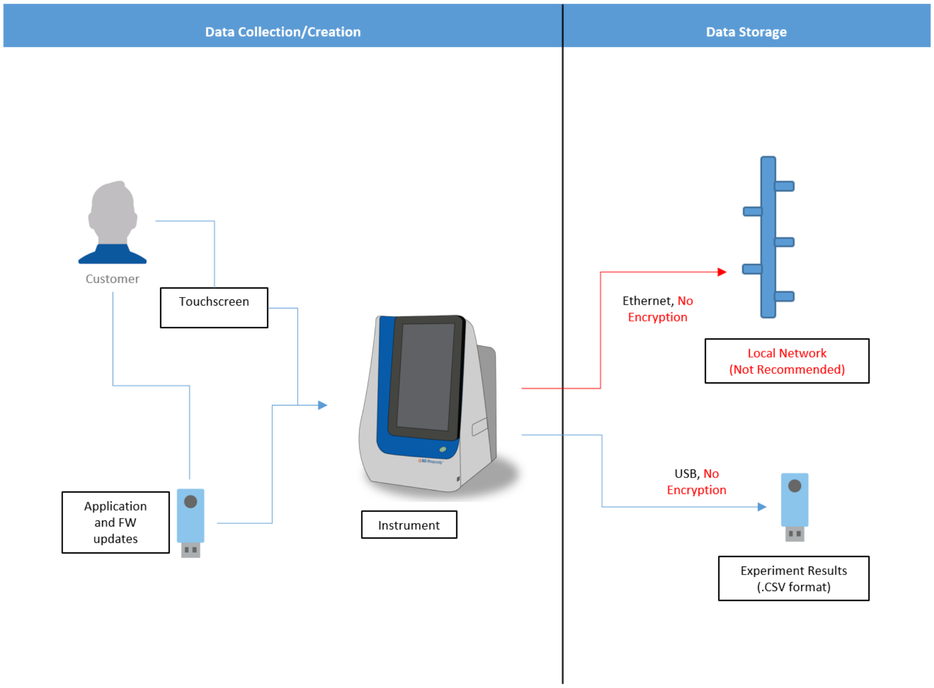
The BD Rhapsody™ Scanner is a Research Use Only (RUO) imaging system and is not designed for use in a clinical environment. The BD Rhapsody™ Scanner Software applications are also not designed for HIPAA compliance. Users are able to enter sensitive data, including PHI/PII, into description fields that are stored in unformatted, plain text. BD recommends that customers use user-generated tracking numbers such as accession numbers or other local data identifiers in place of personal identifiers.

Network and Data Flow Diagram

The diagram below illustrates interactions with the BD Rhapsody™ Scanner for data acquisition and storage. The user primarily interacts via the integrated touchscreen on the Scanner and may apply Application updates using a USB media device. For storage of data, a USB media device is recommended instead of using a local network connection (indicated as Not Recommended below). The BD Rhapsody™ Scanner is not configured for secure connection or encrypted data transmission using the built-in network interface.

NOTE: BD Rhapsody™ Scanner Software v2.0 upgrade requires a hardware upgrade that is not customer installable. A BD Field Service Engineer must install the v2.0 upgrade.

BD Rhapsody™ Scanner – Basic connections



Malware Protection

Microsoft™ Windows™ Defender is configured on the device by default. Other anti-malware solutions or additional compensating controls should not be installed on the device by the customer. BD does not validate specific third-party malware protection solutions for the BD Rhapsody™ Scanner.

Patch Management

Windows™ OS security patches are not provided for the Rhapsody™ Scanner. Windows™ Update features have been disabled in the operating system of the device and it is not recommended for customers to install security patches manually. Devices that malfunction should be returned to BD for service.

Authentication Authorization

The BD Rhapsody™ Scanner has two accounts, a default Administrator account and a RhapsodyUser account. Both accounts have administrative privileges. The software requires administrative permissions to function and is intended to be operated only from the RhapsodyUser account. The administrator account is provided for customer IT or BD Service personnel to recover the system in the event the RhapsodyUser account is disabled.

No customer management of accounts is recommended or supported other than changing of the default password.

Network Controls

The BD Rhapsody™ Scanner is not configured for secure connection or encrypted data transmission using the built-in network interface. The Windows™ Firewall is not configured and the operating system is not hardened. Additional compensating controls should not be installed on the device by the customer.

Encryption

BitLocker™ disk encryption is not verified for use with the BD Rhapsody™ Scanner. BitLocker is not enabled by default in the Windows environment of the BD Rhapsody™ Scanner device.

Audit Logging

BD Rhapsody™ Scanner Software writes the events as noted below to a log file with a date/time stamp. User access to the device is captured in the Windows™ Event logs. Logs of instrument activity can be retrieved by a BD Field Service Engineer (FSE), Field Application Specialist (FAS) or by the customer with instructions provided by a BD FSE or FAS.

- Application logs are located at C:\ProgramData\BD\Rhapsody
- The following information is logged:
  - Application errors and events
  - Application startup
- Systems logs available through the system Event Viewer:
  - Windows systems logins/logouts
  - Windows password changes

  - System errors and events
- Individual Scan and Analysis logs are stored with the experiment data

Remote Connectivity

BD Rhapsody™ Scanner is a standalone device, it does not need to be connected to a network for operation. Windows™ OS-based remote access capability (Remote Desktop) has been disabled for security.

The BD Assurity Linc™ Remote Systems Management Software option for remote service support does not currently support the BD Rhapsody™ Scanner.

Service Handling

The BD Rhapsody™ Scanner Software v2.0 upgrade requires a hardware upgrade that is not customer installable. A BD Field Service Engineer must install the v2.0 upgrade.

Service logs for the instrument and software application can be downloaded from the device by BD Service personnel. These files do not contain user-entered information. For end-of-life devices, BD Service can export Scanner data prior to wiping the internal drive during decommissioning.

Disaster Recovery and Business Continuity

Backup and restore capabilities are not provided for the BD Rhapsody™ Scanner or its data. Data from the Scanner is not used for sample analysis. Scanner results are used as a Quality Control measure for the amount of data that could be generated from the cells in the sample. The Scanner result is discarded once the sample cartridge has moved to the next step in the analysis.

End-of-Life and End-of-Support

BD follows an internal process to provide end-of-life and end-of-support notifications directly to customers, where appropriate. Currently there is no plan for end-of-life or end-of-support for this device and/or service.

Secure Coding Standards

BD Rhapsody™ Scanner Software was not developed to meet specific secure coding standards. BD software coding standards were followed according to the BD internal product development quality process.

System Hardening Standards

Windows™ Firewall is not enabled or configured for the BD Rhapsody™ Scanner. There are no other hardening measures applied to the operating system. The BD Rhapsody™ Scanner device is not configured for network security and should not be connected to the customer network.

Risk Summary

- BD Rhapsody™ Scanner Software is not HIPAA compliant if the user enters PHI/PII data into unformatted descriptive fields for sample-tracking purposes.

  - Mitigation: The customer can use locally generated sample identifiers to avoid using PHI/PII data.
- The BD Rhapsody™ Scanner has a physical network port that is not configured for secure network connections.
  - Mitigation: Connection to the customers network is not supported. Instrument files can be manually backed up to USB media if needed.
- End users with administrative access can install or remove software or execute programs on the device that may introduce or expose vulnerabilities in the system.
  - Mitigation: Administrative access should be strictly controlled by the customer in collaboration with their local IT organization. Installation of other applications is not recommended.
- BD Rhapsody™ Scanner Software does not contain an audit log to assist with adverse event identification.
  - Mitigation: BD expects that the customer will secure the device by limiting physical access or implementing other security controls as the customer sees fit.
- The BD Rhapsody™ Scanner contains three USB ports that could be used to load malicious software.
  - Mitigation: BD expects that the customer will secure the device by limiting physical access or implementing other security controls as the customer sees fit.

Manufacturer's Disclosure Statement for Medical Device Security

Otherwise known as the MDS2 form, this section provides an industry standard convention for security information.

MANUFACTURER DISCLOSURE STATEMENT FOR MEDICAL DEVICE SECURITY -- MDS2			
Manufacturer Name: Becton, Dickinson and Company, BD Biosciences	Device Model: BD Rhapsody™ Scanner	Document ID: **BD-83911**	Document release date: 2023-04-27

	DEVICE DESCRIPTION		
Question ID	Question	Answer	Note #
DOC-1	Manufacturer Name	Becton, Dickinson and Company, BD Biosciences	
DOC-2	Device Description	Imaging scanner for prepared BD Rhapsody™ System single- cell multiomics cartridges	
DOC-3	Device Model	BD Rhapsody™ Scanner	
DOC-4	Document ID	BD-83911	
DOC-5	Manufacturer Contact Information	Becton, Dickinson and Company BD Biosciences 2350 Qume Drive San Jose, CA 95131 For US support: 1-877-232-8995	
DOC-6	Intended use of device in network-connected environment:	Research Use Only device for providing check of BD Rhapsody™ Cartridge.	
DOC-7	Document Release Date	2023-04-27	
DOC-8	Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device?	See Notes	1
DOC-9	ISAO: Is the manufacturer part of an Information Sharing and Analysis Organization?	Yes	
DOC-10	Diagram: Is a network or data flow diagram available that indicates connections to other system components or expected external resources?	See Notes	2
DOC-11	SaMD: Is the device Software as a Medical Device (i.e. software-only, no hardware)?	No	
DOC-11.1	Does the SaMD contain an operating system?	N/A	
DOC-11.2	Does the SaMD rely on an owner/operator provided operating system?	N/A	
DOC-11.3	Is the SaMD hosted by the manufacturer?	N/A	
DOC-11.4	Is the SaMD hosted by the customer?	N/A	
	DEVICE DESCRIPTION – NOTES		
Note 1	Coordinated vulnerability disclosure through the Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Advisories and Reports Program and U.S. Food and Drug Administration, and National Health Information Sharing and Analysis Center (NH-ISAC)		
Note 2	Please refer to this document for a basic diagram.		

	MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION (MPII)	Yes, No, N/A or See Note	Note #

MPII-1	Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))? If yes, provide details or reference in notes.	See Note	1
MPII-2	Does the device maintain personally identifiable information?	No	
MPII-2.1	Does the device maintain personally identifiable information temporarily in volatile memory (i.e., until cleared by power-off or reset)?	No	
MPII-2.2	Does the device store personally identifiable information persistently on internal media?	No	
MPII-2.3	Is personally identifiable information preserved in the device's non-volatile memory until explicitly erased?	No	
MPII-2.4	Does the device store personally identifiable information in a database? If yes, provide details or reference in notes.	No	
MPII-2.5	Does the device allow configuration to automatically delete local personally identifiable information after it is stored to a long term solution?	No	
MPII-2.6	Does the device import/export personally identifiable information with other systems (e.g., a wearable monitoring device might export personally identifiable information to a server)?	No	
MPII-2.7	Does the device maintain personally identifiable information when powered off, or during power service interruptions?	No	
MPII-2.8	Does the device allow the internal media to be removed by a service technician (e.g., for separate destruction or customer retention)?	Yes	
MPII-2.9	Does the device allow personally identifiable information records be stored in a separate location from the device's operating system (i.e. secondary internal drive, alternate drive partition, or remote storage location)?	No	
MPII-3	Does the device have mechanisms used for the transmitting, importing/exporting of personally identifiable information?	No	
MPII-3.1	Does the device display personally identifiable information (e.g., video display, etc.)?	No	
MPII-3.2	Does the device generate hardcopy reports or images containing personally identifiable information?	No	
MPII-3.3	Does the device retrieve personally identifiable information from or record personally identifiable information to removable media (e.g., removable-HDD, USB memory, DVD-R/RW,CD-R/RW, tape, CF/SD card, memory stick, etc.)?	See Note	1
MPII-3.4	Does the device transmit/receive or import/export personally identifiable information via dedicated cable connection (e.g., RS-232, RS-423, USB, FireWire, etc.)?	No	
MPII-3.5	Does the device transmit/receive personally identifiable information via a wired network connection (e.g., RJ45, fiber optic, etc.)?	No	
MPII-3.6	Does the device transmit/receive personally identifiable information via a wireless network connection (e.g., WiFi, Bluetooth, NFC, infrared, cellular, etc.)?	No	
MPII-3.7	Does the device transmit/receive personally identifiable information over an external network (e.g., Internet)?	No	
MPII-3.8	Does the device import personally identifiable information via scanning a document?	No	
MPII-3.9	Does the device transmit/receive personally identifiable information via a proprietary protocol?	No	
MPII-3.10	Does the device use any other mechanism to transmit, import or export personally identifiable information? If yes, provide details or reference in notes.	No	
	MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION (MPII) – NOTES		

Note 1	Rhapsody™ Scanner is a research use only product. It does not have input fields for capturing PHI or PII information. It supports USB media for export of device data however.

	AUTOMATIC LOGOFF (ALOF)	Yes, No, N/A or See Note	Note #
	The device's ability to prevent access and misuse by unauthorized users if device is left idle for a period of time.		
ALOF-1	Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)?	No	1
ALOF-2	Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable?	N/A	
	AUTOMATIC LOGOFF (ALOF) – NOTES		
Note 1	Rhapsody™ Scanner does not have user access control features or provide a screen lock / session lock.		

	AUDIT CONTROLS (AUDT)	Yes, No, N/A or See Note	Note #
	The ability to reliably audit activity on the device.		
AUDT-1	Can the medical device create additional audit logs or reports beyond standard operating system logs?	No	
AUDT-1.1	Does the audit log record a USER ID?	N/A	
AUDT-1.2	Does other personally identifiable information exist in the audit trail?	N/A	
AUDT-2	Are events recorded in an audit log? If yes, indicate which of the following events are recorded in the audit log:	N/A	
AUDT-2.1	Successful login/logout attempts?	N/A	
AUDT-2.2	Unsuccessful login/logout attempts?	N/A	
AUDT-2.3	Modification of user privileges?	N/A	
AUDT-2.4	Creation/modification/deletion of users?	N/A	
AUDT-2.5	Presentation of clinical or PII data (e.g. display, print)?	N/A	
AUDT-2.6	Creation/modification/deletion of data?	N/A	
AUDT-2.7	Import/export of data from removable media (e.g. USB drive, external hard drive, DVD)?	N/A	
AUDT-2.8	Receipt/transmission of data or commands over a network or point-to-point connection?	N/A	
AUDT-2.8.1	Remote or on-site support?	N/A	
AUDT-2.8.2	Application Programming Interface (API) and similar activity?	N/A	
AUDT-2.9	Emergency access?	N/A	
AUDT-2.10	Other events (e.g., software updates)? If yes, provide details or reference in notes.	N/A	
AUDT-2.11	Is the audit capability documented in more detail? If yes, provide details or reference in notes.	N/A	
AUDT-3	Can the owner/operator define or select which events are recorded in the audit log? If yes, provide details or reference in notes.	N/A	
AUDT-4	Is a list of data attributes that are captured in the audit log for an event available? If yes, provide details or reference in notes.	N/A	
AUDT-4.1	Does the audit log record date/time?	N/A	
AUDT-4.1.1	Can date and time be synchronized by Network Time Protocol (NTP) or equivalent time source?	See Notes	2
AUDT-5	Can audit log content be exported?	N/A	

	AUDIT CONTROLS (AUDT)	Yes, No, N/A or See Note	Note #
AUDT-5.1	Via physical media?	N/A	
AUDT-5.2	Via IHE Audit Trail and Node Authentication (ATNA) profile to SIEM?	N/A	
AUDT-5.3	Via Other communications (e.g., external service device, mobile applications)? If yes, provide details or reference in notes.	N/A	
AUDT-5.4	Are audit logs encrypted in transit or on storage media? If yes, provide details or reference in notes.	N/A	
AUDT-6	Can audit logs be monitored/reviewed by owner/operator? If no, provide details or reference in notes.	See Notes	3
AUDT-7	Are audit logs protected from modification? If yes, provide details or reference in notes.	See Notes	3
AUDT-7.1	Are audit logs protected from access? If yes, provide details or reference in notes.	See Notes	3
AUDT-8	Can audit logs be analyzed by the device? If so, provide reference in notes.	N/A	
	AUDIT CONTROLS (AUDT) - NOTES		
Note 1	Rhapsody™ Scanner device does not support user access control, there is no user access log.		
Note 2	Date / Time on the Rhapsody™ Scanner is set manually in the OS.		
Note 3	Event logs in the Windows™ OS are protected from access or modification except by administrators.		

	AUTHORIZATION (AUTH)	Yes, No, N/A or See Note	Note #
	The ability of the device to determine the authorization of users.		
AUTH-1	Does the device prevent access to unauthorized users through user login requirements or other mechanism?	No	
AUTH-1.1	Can the device be configured to use federated credentials management of users for authorization (e.g., LDAP, OAuth)? If yes, provide details or reference in notes.	No	
AUTH-1.2	Can the customer push group policies to the device (e.g., Active Directory)? If yes, provide details or reference in notes.	No	
AUTH-1.3	Are any special groups, organizational units, or group policies required? If yes, provide details or reference in notes.	No	
AUTH-2	Can users be assigned different privilege levels based on 'role' (e.g., user, administrator, and/or service, etc.)?	No	
AUTH-3	Can the device owner/operator grant themselves unrestricted administrative privileges (e.g., access operating system or application via local root or administrator account)?	Yes	1
AUTH-4	Does the device authorize or control all API access requests? If no, provide details or reference in notes.	N/A	
AUTH-5	Does the device run in a restricted access mode, or ‘kiosk mode’, by default? If yes, provide details or reference in notes.	Yes	2
	AUTHORIZATION (AUTH) – NOTES		
Note 1	Rhapsody™ Scanner software must be run with administrator access rights. Only one account (RhapsodyUser) is supported.		
Note 2	Rhapsody™ Scanner device uses Windows™ OS in kiosk mode to hide the OS desktop, but it does not restrict access to it.		

	CYBER SECURITY PRODUCT UPGRADES (CSUP)	Yes, No, N/A or See Note	Note #
	The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade device's security patches.		
CSUP-1	Does the device contain any software or firmware which may require security updates during its operational life, either from the device manufacturer or from a third-party manufacturer of the software/firmware? If no, answer "N/A" to questions in this section.	Yes	
CSUP-2	Does the device contain an Operating System? If yes, complete 2.1-2.4.	Yes	
CSUP-2.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	No	
CSUP-2.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	Yes	
CSUP-2.3	Does the device have the capability to receive remote installation of patches or software updates?	No	
CSUP-2.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	No	
CSUP-3	Does the device contain Drivers and Firmware? If yes, complete 3.1-3.4.	Yes	
CSUP-3.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	No	
CSUP-3.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	Yes	
CSUP-3.3	Does the device have the capability to receive remote installation of patches or software updates?	No	
CSUP-3.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	No	
CSUP-4	Does the device contain Anti-Malware Software? If yes, complete 4.1-4.4.	Yes	
CSUP-4.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	No	
CSUP-4.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	Yes	
CSUP-4.3	Does the device have the capability to receive remote installation of patches or software updates?	No	
CSUP-4.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	No	
CSUP-5	Does the device contain Non-Operating System commercial off-the-shelf components? If yes, complete 5.1-5.4.	No	
CSUP-5.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A	
CSUP-5.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A	
CSUP-5.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A	
CSUP-5.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	N/A	
CSUP-6	Does the device contain other software components (e.g., asset management software, license management)? If yes, please provide details or reference in notes and complete 6.1-6.4.	No	
CSUP-6.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A	

	CYBER SECURITY PRODUCT UPGRADES (CSUP)	Yes, No, N/A or See Note	Note #
CSUP-6.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A	
CSUP-6.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A	
CSUP-6.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	N/A	
CSUP-7	Does the manufacturer notify the customer when updates are approved for installation? If so, provide details or reference it in notes.	See Notes	1
CSUP-8	Does the device perform automatic installation of software updates?	No	
CSUP-9	Does the manufacturer have an approved list of third-party software that can be installed on the device? If so, describe or reference in notes the manufacturer-approved third-party software list and/or the manufacturing process for managing requests to approve additional third-party software.	No	
CSUP-10	Can the owner/operator install manufacturer-approved third-party software on the device themselves?	No	
CSUP-10.1	Does the system have mechanism in place to prevent installation of unapproved software?	No	
CSUP-11	Does the manufacturer have a process in place to assess device vulnerabilities and updates?	Yes	
CSUP-11.1	Does the manufacturer provide customers with review and approval status of updates?	No	
CSUP-11.2	Is there an update review cycle for the device? If so, provide details or reference it in notes.	See Notes	2
	CYBER SECURITY PRODUCT UPGRADES (CSUP) - NOTES		
Note 1	BD provides notification of upgrades when available by customer letter.		
Note 2	Product Security risks are reviewed at the beginning of each development cycle according to BD internal policies and procedures.		

	HEALTH DATA DE-IDENTIFICATION (DIDT)	Yes, No, N/A or See Note	Note #
	The ability of the device to directly remove information that allows identification of a person.		
DIDT-1	Does the device provide an integral capability to de-identify personally identifiable information? If yes, provide details or reference in notes.	No	
DIDT-1.1	Does the device support de-identification profiles that comply with the DICOM standard for de-identification? If so, provide details or reference in notes.	No	
	HEALTH DATA DE-IDENTIFICATION (DIDT) – NOTES		

	DATA BACKUP AND DISASTER RECOVERY (DTBK)	Yes, No, N/A or See Note	Note #
	The ability to recover after damage or destruction of device data, hardware, software, or site configuration information.		
DTBK-1	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)?	No	
DTBK-2	Does the device have a “factory reset” function to restore the original device settings as provided by the manufacturer?	No	

	DATA BACKUP AND DISASTER RECOVERY (DTBK)	Yes, No, N/A or See Note	Note #
DTBK-3	Does the device have an integral data backup capability to removable media?	See Notes	1
DTBK-4	Does the device have an integral data backup capability to remote storage?	See Notes	1
DTBK-5	Does the device have a backup capability for system configuration information, patch restoration, and software restoration? If yes, provide details or reference in notes.	No	
DTBK-6	Does the device provide the capability to check the integrity and authenticity of a backup?	No	
	DATA BACKUP AND DISASTER RECOVERY (DTBK) - NOTES		
Note 1	Rhapsody™ Scanner does not provide a direct sample analysis result. The Scanner assesses the testing cartridge for the amount of data that may be generated from the sampled cells. Integral data backup capability is not provided in the Scanner software.		

	EMERGENCY ACCESS (EMRG)	Yes, No, N/A or See Note	Note #
	The ability of the device user to access personally identifiable information in case of a medical emergency situation that requires immediate access to stored personally identifiable information.		
EMRG-1	Does the device incorporate an emergency access (i.e. “break-glass”) feature? If yes, provide details or reference it in notes.	No	
	EMERGENCY ACCESS (EMRG) - NOTES		

	HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)	Yes, No, N/A or See Note	Note #
	How the device ensures that the stored data on the device has not been altered or destroyed in a non-authorized manner and is from the originator.		
IGAU-1	Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)?	See Notes	1
IGAU-2	Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)?	No	
	HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU) – NOTES		
Note 1	Rhapsody™ Scanner does not provide a direct sample analysis result. The Scanner assesses the testing cartridge for the amount of data that may be generated from the sampled cells. Data integrity checking is not provided.		

	MALWARE DETECTION/PROTECTION (MLDP)	Yes, No, N/A or See Note	Note #
	The ability of the device to effectively prevent, detect and remove malicious software (malware).		
MLDP-1	Is the device capable of hosting executable software?	Yes	
MLDP-2	Does the device support the use of anti-malware software (or other anti-malware mechanism)? Provide details or reference in notes.	See Notes	1
MLDP-2.1	Does the device include anti-malware software by default?	Yes	
MLDP-2.2	Does the device have anti-malware software available as an option?	No	
MLDP-2.3	Does the device documentation allow the owner/operator to install or update anti-malware software? If yes, provide details or reference in notes.	No	
MLDP-2.4	Can the device owner/operator independently (re-)configure anti-malware settings?	Yes	

	MALWARE DETECTION/PROTECTION (MLDP)	Yes, No, N/A or See Note	Note #
MLDP-2.5	Does notification of malware detection occur in the device user interface?	Yes	
MLDP-2.6	Can only manufacturer-authorized persons repair systems when malware has been detected? If yes, provide details or reference in notes.	See Notes	2
MLDP-2.7	Are malware notifications written to a log?	Yes	
MLDP-2.8	Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?	See Notes	4
MLDP-3	If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place or available? If yes, provide details or reference in notes.	N/A	
MLDP-4	Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device? If yes, provide details or reference in notes.	No	
MLDP-5	Does the device employ a host-based intrusion detection/prevention system? If yes, provide details or reference in notes.	No	
MLDP-5.1	Can the host-based intrusion detection/prevention system be configured by the customer?	No	
MLDP-5.2	Can a host-based intrusion detection/prevention system be installed by the customer?	See Notes	5
	MALWARE DETECTION/PROTECTION (MLDP) - NOTES		
Note 1	Windows™ Defender is enabled on the workstation.		
Note 2	If the AV solution cannot remove the virus, Scanner will need to be returned to BD Service Depot for drive reimaging / restoration.		
Note 4	Other anti-malware solutions or additional compensating controls should not be installed on the device by the customer.		
Note 5	Rhapsody™ Scanner device has not been tested with endpoint monitoring or data loss prevention solutions.		

	NODE AUTHENTICATION (NAUT)	Yes, No, N/A or See Note	Note #
	The ability of the device to authenticate communication partners/nodes.		
NAUT-1	Does the device provide/support any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information (e.g. Web APIs, SMTP, SNMP)? If yes, provide details or reference in notes.	No	
NAUT-2	Are network access control mechanisms supported (E.g., does the device have an internal firewall, or use a network connection white list)? If yes, provide details or reference in notes.	No	
NAUT-2.1	Is the firewall ruleset documented and available for review? If yes, provide details or reference in notes.	No	
NAUT-3	Does the device use certificate-based network connection authentication?	No	
	NODE AUTHENTICATION (NAUT) - NOTES		
Note 1	Rhapsody™ Scanner device is not configured for network security. The operating system is not hardened.		

	CONNECTIVITY CAPABILITIES (CONN)	Yes, No, N/A or See Note	Note #
	All network and removable media connections must be considered in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device.		

	CONNECTIVITY CAPABILITIES (CONN)	Yes, No, N/A or See Note	Note #
CONN-1	Does the device have hardware connectivity capabilities? If yes, provide details or a reference that identifies the hardware connectivity capabilities of the device. If no, indicate “none” in notes and answer “N/A” to questions in this section.	Yes	1
CONN-1.1	Does the device support wireless connections?	No	
CONN-1.1.1	Does the device support Wi-Fi? If yes, please list or provide a reference to the Wi-Fi authentication protocols supported (e.g., WPA2 EAP-TLS) in the notes.	No	
CONN-1.1.2	Does the device support Bluetooth? If yes, please list or provide a reference to the Bluetooth security modes supported and indicate if they can be forced in the notes.	No	
CONN-1.1.3	Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? If yes, provide details or reference it in notes.	No	
CONN-1.1.4	Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? If yes, provide details or reference it in notes.	No	
CONN-1.2	Does the device support physical connections?	Yes	
CONN-1.2.1	Does the device have available RJ45 Ethernet ports?	Yes	
CONN-1.2.2	Does the device have available USB ports? If yes, provide details or reference that indicates use and how they are secured in notes.	Yes	2
CONN-1.2.3	Does the device require, use, or support removable memory devices? If yes, provide details or reference it in notes.	Yes	
CONN-1.2.4	Does the device support other physical connectivity? If yes, provide details or reference it in notes.	No	
CONN-2	Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device? If yes, provide details or reference it in notes.	Yes	3
CONN-3	Can the device communicate with other systems within the customer environment? If yes, provide details or reference in notes.	No	
CONN-4	Can the device communicate with other systems external to the customer environment (e.g., a service host)? If yes, provide details or reference in notes.	No	
CONN-5	Does the device make or receive API calls? If yes, provide details or reference in notes.	No	
CONN-6	Does the device require an internet connection for its intended use? If yes, provide details or reference in notes.	No	
CONN-7	Does the device support Transport Layer Security (TLS)? If yes, provide details or reference about supported and prohibited versions of TLS in the notes.	No	
CONN-7.1	Is TLS configurable? If yes, provide details or reference in notes.	N/A	
CONN-8	Does the device provide operator control functionality from a separate device (e.g., telemedicine)? If yes, provide details or reference in notes.	No	
	CONNECTIVITY CAPABILITIES (CONN) - NOTES		
Note 1	Rhapsody™ Scanner has exposed USB and Ethernet ports.		
Note 2	Rhapsody™ Scanner has USB ports enabled for use with storage media for file backup and software upgrade.		
Note 3	See the section Network Ports and Services in this document.		

	PERSON AUTHENTICATION (PAUT)	Yes, No, N/A or See Note	Note #
	The ability to configure the device to authenticate users.		
PAUT-1	Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)?	No	

PAUT-1.1	Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)? If no, provide details or reference in notes.	No	
PAUT-2	Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)? If yes, provide details or reference in notes.	No	
PAUT-3	Is the device configurable to lock out a user after a certain number of unsuccessful logon attempts? If yes, provide details or reference in notes.	No	
PAUT-4	Are all default accounts (e.g., technician service accounts, administrator accounts) listed in the documentation? If no, provide details or reference in notes.	Yes	
PAUT-5	Can all passwords be changed? If no, provide details or reference in notes.	No	
PAUT-6	Is the device configurable to enforce creation of user account passwords that meet established (organization specific) complexity rules? If so, provide details or reference in notes.	No	
PAUT-7	Does the device support account passwords that expire periodically? If yes, provide details or reference in notes.	No	
PAUT-8	Does the device support multi-factor authentication? If yes, provide details or reference in notes.	No	
PAUT-9	Does the device support single sign-on (SSO)? If yes, provide details or reference in notes.	No	
PAUT-10	Can user accounts be disabled/locked on the device?	No	
PAUT-11	Does the device support biometric controls?	No	
PAUT-12	Does the device support physical tokens (e.g. badge access)?	No	
PAUT-13	Does the device support group authentication (e.g. hospital teams)?	No	
PAUT-14	Does the application or device store or manage authentication credentials? If yes, provide details or reference in notes.	No	
PAUT-14.1	Are credentials stored using a secure method? If yes, provide details or reference in notes.	N/A	
	PERSON AUTHENTICATION (PAUT) – NOTES		

	PHYSICAL LOCKS (PLOK)	Yes, No, N/A or See Note	Note #
	Physical locks can prevent unauthorized users with physical access to the device from compromising the integrity and confidentiality of personally identifiable information stored on the device or on removable media		
PLOK-1	Is the device software only? If yes, answer “N/A” to remaining questions in this section.	No	
PLOK-2	Are all device components maintaining personally identifiable information (other than removable media) physically secure (i.e., cannot remove without tools)?	Yes	
PLOK-3	Are all device components maintaining personally identifiable information (other than removable media) physically secured behind an individually keyed locking device?	No	
PLOK-4	Does the device have an option for the customer to attach a physical lock to restrict access to removable media?	No	
	PHYSICAL LOCKS (PLOK) - NOTES		

	ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)	Yes, No, N/A or See Note	Note #

	Manufacturer's plans for security support of third-party components within the device's life cycle.		
RDMP-1	Was a secure software development process, such as ISO/IEC 27034 or IEC 62304, followed during product development? If yes, provide details or reference in notes.	Yes	1
RDMP-2	Does the manufacturer evaluate third-party applications and software components included in the device for secure development practices?	Yes	
RDMP-3	Does the manufacturer maintain a web page or other source of information on software support dates and updates? If yes, provide details or reference in notes.	No	
RDMP-4	Does the manufacturer have a plan for managing third-party component end-of-life? If yes, provide details or reference in notes.	Yes	2
	ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP) - NOTES		
Note 1	BD software product development process is aligned with IEC 62304 and includes secure code analysis to identify findings based on industry standards.		
Note 2	Third-party components are reviewed for vulnerabilities and end-of-life with each release cycle. Findings are documented in the Product Security Management plan for the product.		

	SOFTWARE BILL OF MATERIALS (SBoM)	Yes, No, N/A or See Note	Note #
	A Software Bill of Material (SBoM) lists all the software components that are incorporated into the device being described for the purpose of operational security planning by the healthcare delivery organization. This section supports controls in the RDMP section.		
SBOM-1	Is the SBoM for this product available? If yes, provide details or reference in notes.	See Notes	1
SBOM-2	Does the SBoM follow a standard or common method in describing software components? If yes, provide details or reference in notes.	See Notes	1
SBOM-2.1	Are the software components identified?	Yes	
SBOM-2.2	Are the developers/manufacturers of the software components identified?	Yes	
SBOM-2.3	Are the major version numbers of the software components identified?	Yes	
SBOM-2.4	Are any additional descriptive elements identified? If yes, provide details or reference in notes.	No	
SBOM-3	Does the device include a command or process method available to generate a list of software components installed on the device? If yes, provide details or reference in notes.	No	
SBOM-4	Is there an update process for the SBoM? If yes, provide details or reference in notes.	Yes	2
	SOFTWARE BILL OF MATERIALS (SBoM) – NOTES		
Note 1	Please refer to the table of 3rd party software and OS components in this document.		
Note 2	The list of 3rd party components is reviewed and updated for each product release.		

	SYSTEM AND APPLICATION HARDENING (SAHD)	Yes, No, N/A or See Note	Note #
	The device's inherent resistance to cyber attacks and malware.		
SAHD-1	Is the device hardened in accordance with any industry standards? If yes, provide details or reference in notes.	No	1
SAHD-2	Has the device received any cybersecurity certifications? If yes, provide details or reference in notes.	No	
SAHD-3	Does the device employ any mechanisms for software integrity checking	No	

	SYSTEM AND APPLICATION HARDENING (SAHD)	Yes, No, N/A or See Note	Note #
SAHD-3.1	Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?	No	
SAHD-3.2	Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-authorized updates?	No	
SAHD-4	Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)? If yes, provide details or reference in notes.	No	
SAHD-5	Is the system configurable to allow the implementation of file-level, patient level, or other types of access controls?	No	
SAHD-5.1	Does the device provide role-based access controls?	No	
SAHD-6	Are any system or user accounts restricted or disabled by the manufacturer at system delivery? If yes, provide details or reference in notes.	No	
SAHD-6.1	Are any system or user accounts configurable by the end user after initial configuration?	No	
SAHD-6.2	Does this include restricting certain system or user accounts, such as service technicians, to least privileged access?	No	
SAHD-7	Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled? If yes, provide details or reference in notes.	No	
SAHD-8	Are all communication ports and protocols that are not required for the intended use of the device disabled? If yes, provide details or reference in notes.	No	
SAHD-9	Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the intended use of the device deleted/disabled? If yes, provide details or reference in notes.	No	
SAHD-10	Are all applications (COTS applications as well as OS-included applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device deleted/disabled? If yes, provide details or reference in notes.	No	
SAHD-11	Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)? If yes, provide details or reference in notes.	No	
SAHD-12	Can unauthorized software or hardware be installed on the device without the use of physical tools? If yes, provide details or reference in notes.	Yes	
SAHD-13	Does the product documentation include information on operational network security scanning by users? If yes, provide details or reference in notes.	No	
SAHD-14	Can the device be hardened beyond the default provided state?	No	
SAHD-14.1	Are instructions available from vendor for increased hardening? If yes, provide details or reference in notes.	No	
SHAD-15	Can the system prevent access to BIOS or other bootloaders during boot?	No	
SAHD-16	Have additional hardening methods not included in 2.3.19 been used to harden the device? If yes, provide details or reference in notes.	No	
	SYSTEM AND APPLICATION HARDENING (SAHD) – NOTES		
Note 1	Rhapsody™ Scanner operating system has not been hardened to comply with DISA STIGs.		

	SECURITY GUIDANCE (SGUD)	Yes, No, N/A or See Note	Note #
	Availability of security guidance for operator and administrator of the device and manufacturer sales and service.		
SGUD-1	Does the device include security documentation for the owner/operator? If yes, provide details or reference in notes.	No	
SGUD-2	Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media? If yes, provide details or reference in notes.	No	
SGUD-3	Are all access accounts documented?	Yes	
SGUD-3.1	Can the owner/operator manage password control for all accounts?	No	
SGUD-4	Does the product include documentation on recommended compensating controls for the device?	No	
	SECURITY GUIDANCE (SGUD) – NOTES		

	HEALTH DATA STORAGE CONFIDENTIALITY (STCF)	Yes, No, N/A or See Note	Note #
	The ability of the device to ensure unauthorized access does not compromise the integrity and confidentiality of personally identifiable information stored on the device or removable media.		
STCF-1	Can the device encrypt data at rest? If yes, provide details or reference in notes.	No	
STCF-1.1	Is all data encrypted or otherwise protected? If yes, describe or provide a reference in notes.	N/A	
STCF-1.2	Is the data encryption capability configured by default?	N/A	
STCF-1.3	Are instructions available to the customer to configure encryption?	N/A	
STCF-2	Can the encryption keys be changed or configured? If yes, describe or provide a reference in notes.	No	
STCF-3	Is the data stored in a database located on the device? If yes, describe or provide a reference in notes.	No	
STCF-4	Is the data stored in a database external to the device? If yes, describe or provide a reference in notes.	No	
	HEALTH DATA STORAGE CONFIDENTIALITY (STCF) – NOTES		

	TRANSMISSION CONFIDENTIALITY (TXCF)	Yes, No, N/A or See Note	Note #
	The ability of the device to ensure the confidentiality of transmitted personally identifiable information.		
TXCF-1	Can personally identifiable information be transmitted only via a point-to-point dedicated cable?	See Notes	1
TXCF-2	Is personally identifiable information encrypted prior to transmission via a network or removable media? If yes, describe or provide a reference in notes.	N/A	
TXCF-2.1	If data is not encrypted by default, can the customer configure encryption options?	N/A	
TXCF-3	Is personally identifiable information transmission restricted to a fixed list of network destinations?	N/A	
TXCF-4	Are connections limited to authenticated systems? If yes, describe or provide a reference in notes.	N/A	

TXCF-5	Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)? If yes, describe or provide a reference in notes.	N/A	
	TRANSMISSION CONFIDENTIALITY (TXCF) - NOTES		
Note 1	Rhapsody™ Scanner does not have wireless networking capability. There is no PII data in the system.		

	TRANSMISSION INTEGRITY (TXIG)	Yes, No, N/A or See Note	Note #
	The ability of the device to ensure the integrity of transmitted data.		
TXIG-1	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission? If yes, describe or provide a reference in notes.	No	
TXIG-2	Does the device include multiple sub-components connected by external cables? If yes, describe or provide a reference in notes.	No	
	TRANSMISSION INTEGRITY (TXIG) - NOTES		
Note 1	Rhapsody™ Scanner does not transmit data to another system. There is no PII data in the system.		

	REMOTE SERVICE (RMOT)	Yes, No, N/A or See Note	Note #
	Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.		
RMOT-1	Does the device permit remote service connections for device analysis or repair? If yes, describe or provide a reference in notes.	No	
RMOT-1.1	Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?	N/A	
RMOT-1.2	Is there an indicator for an enabled and active remote session?	N/A	
RMOT-1.3	Can patient data be accessed or viewed from the device during the remote session?	N/A	
RMOT-2	Does the device permit or use remote service connections for predictive maintenance data? If yes, describe or provide a reference in notes.	No	
RMOT-3	Does the device have any other remotely accessible functionality (e.g. software updates, remote training)? If yes, describe or provide a reference in notes.	No	
	REMOTE SERVICE (RMOT) - NOTES		

	OTHER SECURITY CONSIDERATIONS (OTHR)
	NONE

Disclaimer

The information contained in this Product Security White Paper is for reference purposes only. Nothing contained in this document or relayed verbally to any customer will be deemed to amend, modify or supersede the terms and conditions of any written agreement between such customer and BD, or BD's subsidiaries or affiliates (collectively, "BD"). BD does not make any promises or guarantees to customer that any of the methods or suggestions described in this Product Security White Paper will restore customer's systems, resolve any issues related to any malicious code or achieve any other stated or intended results. Customer exclusively assumes all risk of utilizing or not utilizing any guidance described in this Product Security White Paper, and customer agrees to indemnify and hold BD harmless from the same.

For Research Use Only. Not for use in diagnostic or therapeutic procedures.