Product Security White Paper

BD Remote Support Services (RSS)

BD is committed to providing secure products to our customers given the important benefits they provide to patient health. 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, 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's 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 Remote Support Services, 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 Remote Support Services (RSS) solution allows BD to remotely support and manage BD products. The BD Remote Support Services Platform is comprised of components that perform the following major functions:

Non-Department of Defense Customers:

- Remote Access
- Remote Monitoring
- Remote Package Deployment
- Remote Management of Microsoft Patches
- Remote Management of Antivirus
- Customer Audit Reports
- Remote software installation and configuration

DoD Customers:

- Remote Access
- Remote Management of Microsoft Patches

See RSS Supported BD Products section below for applicable products.

The functions of the RSS Platform are performed through an interactive web application.

RSS is a scalable cloud-based platform for BD to launch and manage products deployed around the globe.

- Minimizes product downtime through remote management and proactive monitoring.
- Simplify product implementation through integrated mass software updates.
- Manage product security compliance

- Environment or Ecosystem: RSS and Remote Implementation Platform:
  - Microsoft Azure
- BeyondTrust – (previously known as Bomgar) Infrastructure (Remote Desktop Platform)

  - Hosted and managed by BD
- RSS and Remote Implementation Agent
  - See RSS Supported RSS Supported BD Products section, page 12, below for applicable products
- Microsoft Windows WSUS
  - Hosted and managed by BD
- ESET PROTECT PLATFORM
  - Hosted and managed by BD

Operating Systems

- Server: RSS Platform
  - Microsoft Azure Data Center
- Client: RSS deploys lightweight agents that run on BD devices.
  - See RSS Supported RSS Supported BD Products section, page 12, below for applicable products

Third-party Software

Client: RSS deploys lightweight agents that run on BD devices.

- SQLite
- VistaDB
- Microsoft SQL Server Compact.

Server: The RSS Platform is built using Microsoft Azure cloud services. These services include:

- Microsoft Azure Web services
- Microsoft Azure Databases
- Microsoft Azure Identity
- Microsoft Azure Networking
- Microsoft Azure Storage
- Microsoft Azure Security

Remote Access:

- BeyondTrust – (previously known as Bomgar)
- BeyondTrust – (previously known as Bomgar) Jump Client

Network Ports and Services

RSS and Windows Server Update Services (WSUS) Agents:

- All communication out of institution network is done through port 443 (Outbound/Egress)
- Package metadata for WSUS transmitted over port 80
- ESET ® Antivirus metadata transmitted over port 443

- Data received into the institution network is done through port 443

*Department of Defense only: DOD specific infrastructure for WSUS and BeyondTrust (previously known as Bomgar) communication remain the same. There is no outbound traffic from RSS agents for the purpose of monitoring and package deployment.

Sensitive Data Transmitted

RSS does not transfer any electronic Protected Health Information (ePHI) as a part of routine support procedures. In the event RSS collects any sensitive data from a device while service is being performed, RSS transmits such information over a secure connection and maintains it on an encrypted data store (Data stored uses Azure SQL TDE/AES256). The RSS system only retains this type of data for the duration of the specific support session.

Remote sessions have the potential to display the following information on a support technicians' desktop:

- Demographics (e.g., name, address, date of birth, location, unique identification number)
- Medical record (e.g., medical record #, account #, test or treatment date, device identification number).
- Remote screen sharing session information is not recorded or stored.

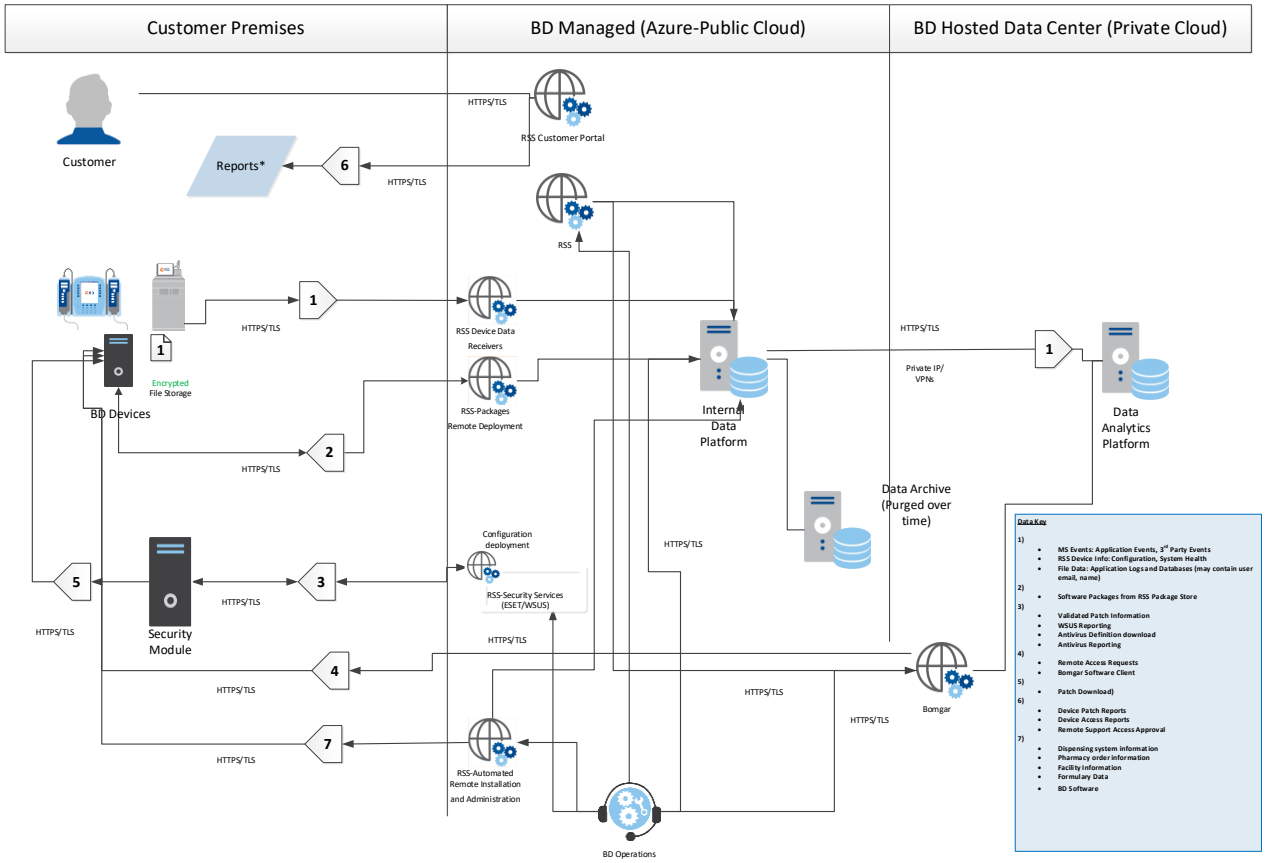
Sensitive Data Stored

- Remote Access: None
- Remote Monitoring: None
- Remote Package Deployment: None
- Remote Management of Microsoft Patches: None
- Remote Management of Antivirus: None
- Customer Audit Reports: Usernames and Email Addresses

Network and Data Flow Diagram

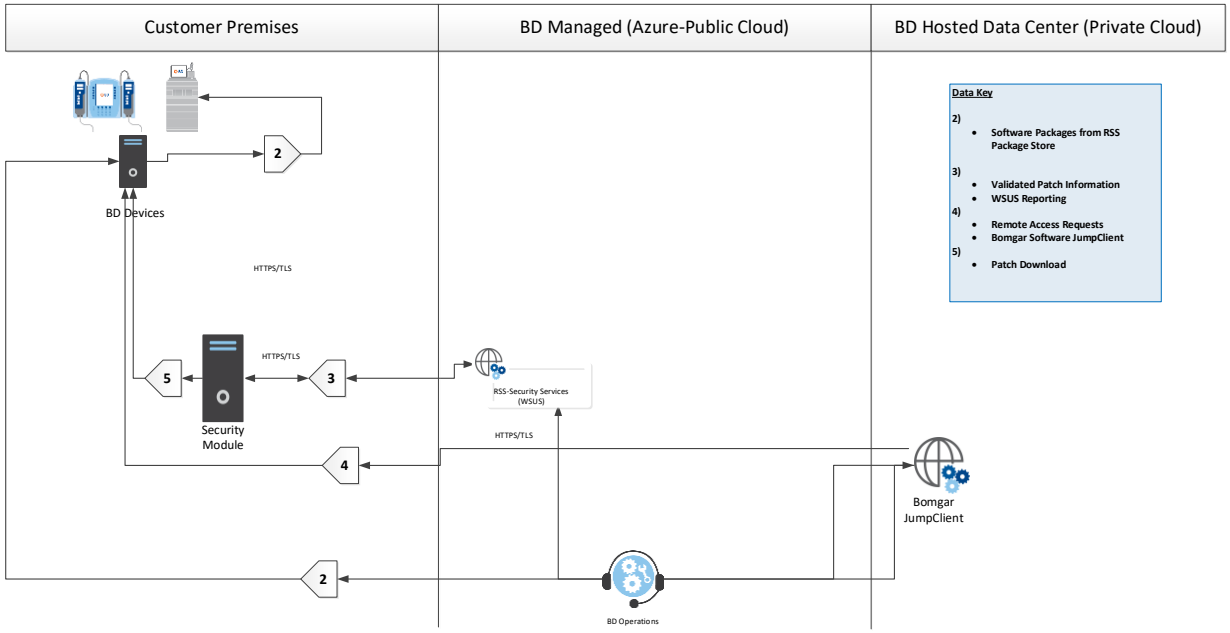
BD Remote Support Services and Automate Remote Installation and Administration (ARIA) Network Architecture:

Commercial Customers



[Space Intentionally Left Blank]

DoD Customers



[Space Intentionally Left Blank]

Malware Protection

RSS Malware Protection in Azure:
RSS is a Platform-as-a-Service (PaaS) solution and Microsoft is responsible for malware protection of the underlying system.

Patch Management

BD proactively monitors and manages Microsoft patching for the applications' hosted environment accordingly:

- Medium to Critical Risks: Patches must be applied within 30 days after initial discovery.
- Low Risks: May be addressed separately in a reasonable amount of time however, at a minimum, during the next product or software update.

Note: RSS is a PaaS solution and Microsoft is responsible for patching underlying system.
DOD:
The Security Compliance Solution is not used in the DOD environment; instead, DOD's Host Based Security System (HBSS) is used for performing cybersecurity protection services on BD devices.
RSS Patching Services:
Additionally, RSS provides a patching service to BD devices deployed to customer premises. RSS supports BD devices that are Windows based by providing Windows Security Updates that can be applied via Microsoft WSUS. Patch updates are reviewed and tested before being approved for deployment by each of the platforms supported via RSS. Upon approval, BD works with individual facilities to coordinate the deployment of the patches for each of the platforms. Patch management configuration for enabling automatic installation, reboots, and update time are discussed during implementation.

See RSS Supported RSS Supported BD Products section (page 12) below for applicable products.

Authentication Authorization

RSS Portal:

The RSS Portal authenticates BD associates (RSS users) against a Microsoft Active Directory instance that is maintained by BD. RSS users are authenticated via Active Directory Federation Services (ADFS). By utilizing these authentication methods, the system maintains unique user credentials, requires strict password protocols, and enforces periodic password changes. As a result, BD associates who require access to RSS must first obtain a BD account via an employee onboarding process. Once a new BD associate has been granted an account, their direct management must provide additional training—including ePHI handling and authorization prior to receiving access to RSS. BD maintains an audit log of all BD associates who have been granted access and completed the appropriate training. If a BD associate leaves BD, BD suspends their account within 24 hours as a part of its standard off-boarding procedures.

In addition, BD associates working off-site require multi-factor authentication through a secure VPN connection to access RSS on the BD network.

RSS Customer Portal:
Users must be granted permissions by the facility through a registration and onboarding process that validates the registration information provided.

Remote Access Authorization:
Through RSS Customer Portal, customers are provided an additional layer of control by optionally requiring a secondary approval of remote access requests during the time of the troubleshooting session. This method can be useful for sensitive devices that customers want more visibility to whom and when devices are being accessed. Patching approval:

Patching approval is tested and released through a controlled process managed through the RSS portal. The approval process is audited at each stage of the process and can only be performed by users with appropriate permissions in RSS.

Network Controls

Most devices connected to the Internet are not directly accessible externally from outside of an organization's private IT network. To prevent unauthorized access, IT network administrators prefer that their computers and devices are protected from the outside world behind secure firewalls, routers and proxy servers. This enables users within the facility to access the internet while helping to prevent unauthorized persons or applications from gaining visibility or access to the computers within the facility.

BD's access to devices at the facility is restricted to BD devices running RSS Agents. RSS works within these boundaries by using a communication protocol that permits remote devices to exchange information with hosted RSS enterprise servers, even when devices are behind corporate firewalls or proxy servers. This technology for device-initiated communications is based on standard Hypertext Transfer Protocol Secure (HTTPS). With RSS, remote systems and devices initiate all secure communications with an enterprise server at a globally visible Internet address. This enables devices to be deployed in many environments without requiring any modification of security settings within the local network environment. As a result, if a web browser can access the internet using a TLS 1.2 network connection, the RSS-enabled device will be able to perform secure two-way communications with the enterprise server using the same network connection.
This method of communication:

- Leverages the existing security infrastructure at the device location. The device receives the same network security coverage as all other computers within your facility.
- Simplifies device deployment. Your local IT staff often does not need to make any changes to their existing security configuration. When they connect the device to the local network, it is ready to communicate.

Note: For facilities that employ web filtering, the RSS servers should be white listed for proper operation.

- Helps mitigate the possibility of unauthorized access since the device initiates all communication to a specified server from within the hospitals network and does not possess a public IP address that an attacker would potentially exploit to gain access to the device.
- Our solution offers the possibility for egress filtering, the practice of monitoring and potentially restricting the flow of information outbound from one network to another.

The BD Technical Support Center does not share login accounts for remote support. Each user has a unique account into the RSS platform. The password is based on the BD Active Directory and is changed every 90 days or more frequently. The application uses an industry standard encryption to store and transmit all user passwords. BD IT requires a minimum of eight (8) characters for the password length and synchronizes all users with BD Active Directory, known as Lightweight Directory Access Protocol (LDAP). RSS permits three failed login attempts before the user is locked out for 30 minutes.

DOD:

RSS agents are not installed on BD devices deployed in DOD institutions and do not send data back to the RSS Platform.

Encryption

All communication by RSS happens via Transport Layer Security (TLS) over TCP port 443 (outbound rule only). The RSS Dashboard supports TLS versions 1.2 – 1.0 starting with 1.2 based on client configuration. The RSS agent negotiates the connection protocol with the RSS Dashboard based on local OS settings which will vary based on the BD product. Remote access sessions made into remoteaccess-rss.carefusion.com are established using TLS 1.2.

The RSS TLS tunnel leverages industry standard ciphers negotiated between the remote device and the hosted BD RSS services.

RSS.bd.com = AES 256, SHA384 with RSA 3072 bits/TLS 1.2
RSS.carefusion.com = AES 256, SHA384 with RSA 3072 bits/TLS 1.2
Aria.carefusion.com = AES 256, SHA384 with RSA 3072 bit/TLS 1.2
Aria-api.carefusion.com = AES 256, SHA384 with RSA 3072 bit/TLS 1.2
Remoteaccess-rss.carefusion.com = AES 256, SHA384 with RSA 3072 bit/TLS 1.2
Installportal.bd.com = AES 256, SHA384 with RSA 3072 bit/TLS 1.2

DOD:
Bomgar clients communicate with the Bomgar server using SHA1 encryption.

Audit Logging

The RSS enterprise server electronically logs user identification, date and time, and device ID anytime an authenticated user initiates remote access, file transfer or software distribution. These logs are archived for up to 7 years in order to meet customer audit requests.

Through RSS Customer Portal, customers can additionally audit remote access to BD devices.

Remote Connectivity

BD Remote Support Services (RSS) is BD's remote connectivity solution.

Service Handling

Service handling of the RSS infrastructure is performed by BD Data Center Operations. BD has an access management process in place to request, approve, and review access to production environments. BD associates must take ePHI handling and authorization training as a pre-requisite to gaining access. In the event an employee leaves BD or transfers to a different position, BD removes their access. BD maintains an audit log of all users (customer and employee). Please see the Patch Management, Network Controls, and Authentication and Authorization sections for further information on those topics.

DOD: BD associates must secure Government Security Clearance before being approved by BD for access to BD devices deployed in DOD institutions.

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 as necessary. Currently there is no plan to end-of-life or end-of-support these applications.

Secure Coding Standards

Fortify on Demand is used as the static code analysis tool for these applications. The following secure coding standards are adhered to during development of these applications:

- OWASP Top 10 threats
- Microsoft Security Checklist (Web, .NET, Database)

System Hardening Standards

The following standards and guidelines are used in the software development and operational procedures used to support the production environments:

- FDA Cybersecurity Guidelines
- NIST SP 800-53 Rev. 4
- DISA STIG
- HIPAA Privacy & Security Rules
- NSA Guides
- OWASP Top 10
- CIS

RSS Supported BD Products

BD Product	Remote Access	Monitoring	Package Deployment	Windows patch configuration and reporting	Antivirus configuration and reporting	Remote access Audit Reports	Remote Software Installation
BD Pyxis™ ES System **	X	X	X	X	X	X	X
BD Pyxis™ MedStation™ 4000 System **	X	X	X	X	X	X	X
BD Pyxis™ MedStation™ 3500 System **	X	X	X	X	X	X	X
BD Pyxis™ MedStation™ 3000 System	X	X	X	X	X	X	X
BD Pyxis™ Logistics **	X	X	X	X	X	X	X
BD Pyxis™ Check	X	X	X	X	X	X	X
BD Pyxis™ Order Viewer	X	X	X	X	X	X	X
BD Pyxis™ IV Prep (US Only) ** BD Cato™ (EU Only)	X	X	X	X	X	X	X
BD Pyxis™ CIISafe **	X	X	X	X	X	X	X
BD Pyxis™ SupplyStation™ **	X	X	X	X	X	X	X
BD Pyxis™ SupplyCenter **	X	X	X	X	X	X	X
BD Pyxis™ SupplyCenter VM **	X	X	X	X	X	X	X
BD Alaris™ System	X	X	X	X	X	X	X

BD Product	Remote Access	Monitoring	Package Deployment	Windows patch configuration and reporting	Antivirus configuration and reporting	Remote access Audit Reports	Remote Software Installation
Manager Server **							
Pyxis™ PARx™	X	X	X	X	X	X	X
BD Rowa™ Dose (US Only)	X	X	X		X	X	
BD Care Coordination Engine (CCE) **	X	X	X	X	X	X	X
Security Module **	X	X	X	X	X	X	X
MedMined™ services	X	X				X	
BD FACSAria™ II	X	X				X	
BD FACSAria™ III	X	X				X	
BD FACSAria™ Fusion	X	X				X	
BD FACSCanto™ A	X	X				X	
BD FACSCanto™ II	X	X				X	
BD FACSCanto™ 10-color	X	X				X	
BD FACSCelesta™	X	X				X	
BD FACSLink™	X	X				X	
BD FACSLyric™	X	X				X	
BD FACSLyric™ - R	X	X				X	
BD FACSMelody™	X	X				X	
BD LSR II	X	X				X	
BD LSRFortessa™	X	X				X	
BD LSRFortessa™ X-20	X	X				X	

BD Product	Remote Access	Monitoring	Package Deployment	Windows patch configuration and reporting	Antivirus configuration and reporting	Remote access Audit Reports	Remote Software Installation
BD FACSymphony™	X	X				X	
BD FACSVerse™	X	X				X	
BD EpiCenter™	X	X				X	
BD MAX™	X	X				X	
BD Kiestra™	X	X				X	
BD Totalys™	X	X				X	
BD Viper™ LT	X	X				X	
BD BACTEC™ FX, FX40	X	X				X	
BD Viper™ XTR	X	X				X	
BD Synapsys™	X	X				X	
BD Phoenix™ M50	X	X				X	

Risk Summary

The following vulnerabilities were revealed and should be considered for installation planning and operational procedures:

- The following web portals in the RSS platform do not support MFA. These areas use BD Azure AD username password-based authentication. Note: All areas of RSS Platform are monitored periodically for auditing purposes:
  - rss.bd.com
  - Remoteaccess-rss.carefusion.com
  - installportal.bd.com
  - aria.carefusion.com
- RSS stores all credential data encrypted when at rest but may store credential data unencrypted in-memory while in use.
  - Access to memory requires elevated privileges (i.e. Administrator access, and/or physical access) to the device and to the BD devices.
- RSS supports TLS 1.2. Some older devices that leverage older operating systems may not support TLS 1.1 or 1.2.
  - Refer to core product (e.g. Pyxis, Alaris) security whitepaper for further information on compensating controls for this risk.
- RSS Concurrent User Access: RSS allows users to access from multiple devices

  - The RSS portal accessed by BD associates require they are on the BD corporate network before doing so. (Note: BD Associates my remotely access the BD corporate network via VPN in order to access RSS portal.)
- The system supports certificate authorization between RSS agents and server. It does not support client-side authorization such as certificate pinning.
  - Devices that connect to RSS are located within institution networks and present limited risk as a result. Additionally, the RSS portal accessed by BD associates require they are on the BD corporate network before doing so.
- Hardcoded Cryptographic keys are used to both encrypt and decrypt various credentials and secrets used in various functions.
  - Permissions give to RSS Agent are used as a service account and are not exposed to users at the institution. Devices that connect to RSS are located within institution networks and present limited risk as a result. Additionally, the RSS portal accessed by BD associates require they are on the BD corporate network before doing so and all activities are logged.

Third Party Soc2+ Reporting

Our commitment to ongoing Service Organization Control (SOC) Type II Plus reporting enhances the transparency of our relationship with customers. This reporting allows for visibility into the policies, procedures and processes governing the use of data gathered from customer environments.

Using an independent third party, we annually test and report on the operating effectiveness of controls in relation to the trust services principles & criteria for security and availability, as well as NIST800-66 (An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule). The third party firm completes their reporting in alignment with the American Institute of Certified Public Accountants (AICPA) over the suitability of the design and operating effectives of controls to meet the applicable criteria.

As part of this year's annual review, the following areas will be assessed:

1. Security Management Process
2. Security Official
3. Workforce Security
4. Information Access Management
5. Security Awareness and Training
6. Security Incident Procedures
7. Contingency Plan
8. Evaluation
9. Business Associate Contracts and Other Arrangements
10. Facility Access Controls
11. Workstation Use
12. Workstation Security
13. Device and Media Controls
14. Access Controls
15. Report Controls
16. Integrity
17. Person or Entity Authentication
18. Transmission Security
19. Business Associate Monitoring Process
20. Policies and Procedures

Manufacturer's Disclosure Statement for Medical Device Security

BD RSS is not a regulated Medical Device nor is it software that runs on a medical device. As a result, this section has been left empty.

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.

Revision History

Rev	Revision Description	Rationale for Change	Author
01	Initial Release	N/A	Willis Lam
02	Updated with new Products supported by BD Remote Support Services; eg BD Biosciences products.	Updates	Willis Lam
03	Updated to latest Whitepaper Template, updated risk section with findings from penetration test, updated Network Diagram	Updates	Willis Lam
04	Updated Encryption section, added additional “Remote software installation and configuration” information.	Updates	Willis Lam
05	Updated document to not have TrackChanges information.	Updates	Willis Lam
06	Updated Risk Section with customer findings, and changes to Multifactor. Updated data flow to reflect new ES features that support device migration using RSS. Removed ®, and ™ from Microsoft and Azure	Updates	Willis Lam