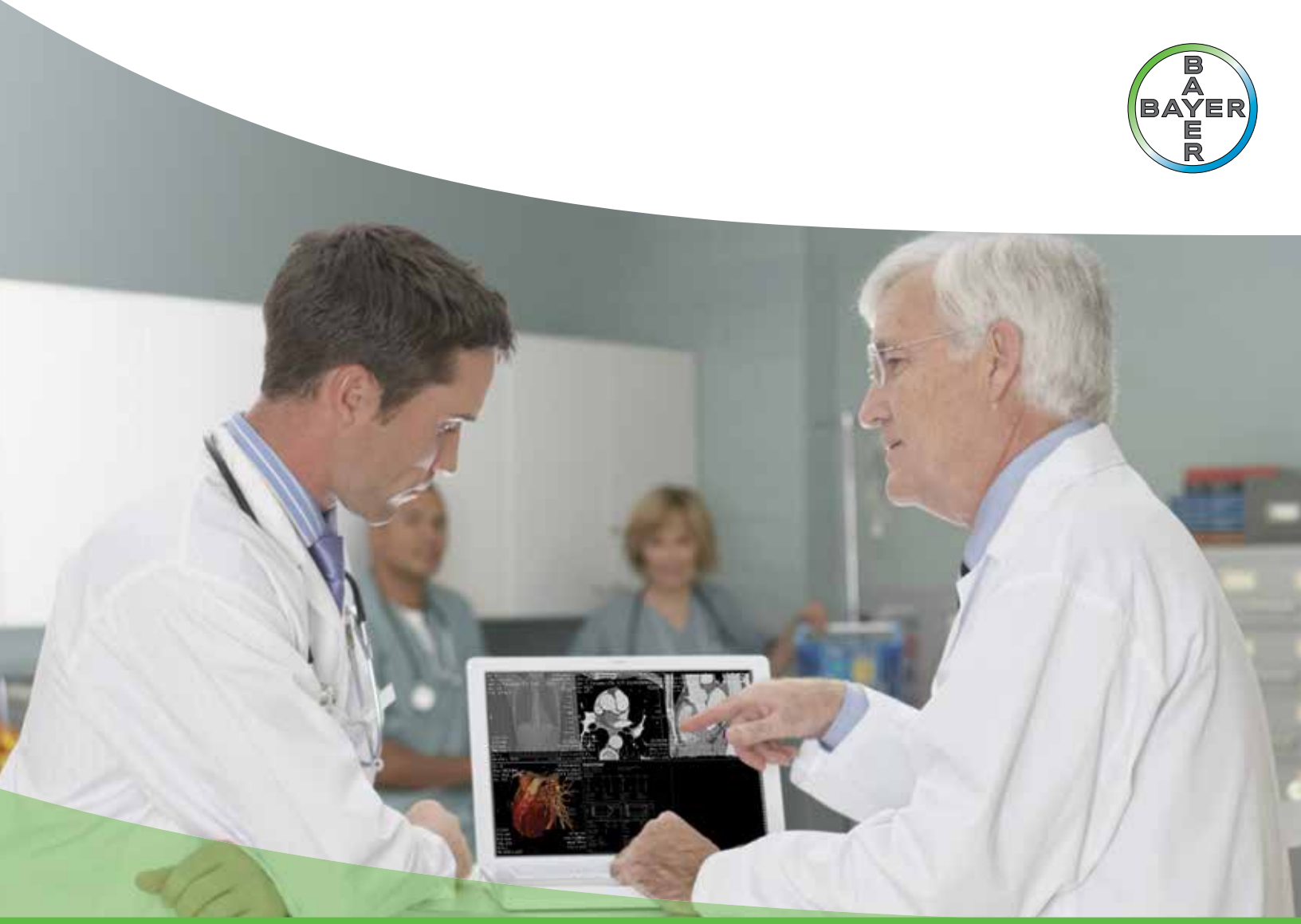

VirtualCare® Remote Support

Technology and Security
White Paper for IT Managers

VirtualCare®
Remote Support

VirtualCare®
Remote Support

VirtualCare® Remote Support allows advanced remote troubleshooting capabilities and system updates through remote services and standard technologies which have been relied on for years in industries such as banking and financial services. This document is for the benefit of Bayer customers, in particular IT managers and administrators, and describes the configuration, security and technology leveraged for VirtualCare® Remote Support.

Overview

VirtualCare® Remote Support allows Bayer to remotely service the devices installed behind customer firewalls securely, over the Internet. The solution leverages secure web services to communicate over the Internet and links the VirtualCare enabled device to a central *Server* hosted by PTC Inc's ISO/IEC 27001:2005 data centers. The solution has been designed for high performance and security at every level of its architecture with a goal to provide faster overall recovery time and maximize uptime of Bayer products. Faster response time through remote diagnostics, increased first-time fix rate through diagnosis before dispatch and immediate access to latest product software and enhancements through remote software updates are a few of the benefits made possible by VirtualCare Remote Support.

VirtualCare is powered by remote connectivity technology from PTC Inc, the same technology being used byleading manufacturers of medical and diagnostic imaging equipment to provide remote service and monitoring at hospitals, clinics and laboratories all over the world.

Components

VirtualCare leverages two major technical components – the *Agent* that is installed on the VirtualCare enabled device deployed at a customer site and the *Server* that resides within Bayer's support center. The *Agent*, a software module that runs on the VirtualCare enabled device, establishes a secure on demand HTTPS (ports 443, 17001, 17002, 80, 8080) connection to the *Server* via the Internet to enable service diagnostic communications. The *Server* is the management console for VirtualCare that allows our service team professionals to run diagnostics remotely and set up software updates for distribution.

Configuration

The *Agent* makes connections to Bayer from behind the safety of the customer's corporate firewall, adhering to all security policies set up by the customer's network administrators. The only requirement is to allow outbound Internet access for ports 443, 17001, 17002, 80 & 8080.

Network Security

Bayer's goal is to support the customer's existing network standards and security practices. A transparent, secure, three layer security architecture based on Web Services is used to accommodate the facility firewall and internal policies in order to enable remote connectivity. The architecture employs security at the device, network, and enterprise layers built using technology specifically designed for secure, efficient Intelligent Device Management (IDM) communications. This includes a hardened software design for application security with support for widely used industry standards such as TCP/IP, HTTPS, SOAP, and XML.

Conclusion

In summary, VirtualCare was designed to provide an advanced, yet acceptable, means of secure remote support for Bayer equipment. Understanding the need to protect against network risks, VirtualCare® Remote Support utilizes the same technology being used by leading manufacturers of medical and diagnostic imaging equipment to provide remote service and monitoring at hospitals, clinics, and laboratories all over the world.

The VirtualCare solution does not store or display any patient protected health information within the central Server

		IP Address	Hostname	Port 443	Port 17001	Port 17002	Port 80	Port 8080
Radimetrics		64.250.188.50	subversion.assembla.com	X			X	
		184.106.132.50	supportserver.radimetrics.com	X			X	X
		5.79.17.149	uksupportserver.radimetrics.com	X			X	X
	Fluid Delivery Devices	209.202.167.124	medrad.axeda.com	X	X	X		
		52.8.82.253	ghsj1.axeda.com	X	X	X		
		209.202.157.179	ghsom1.axeda.com	X	X	X		
		122.202.65.179	Gas-aus.axeda.com	X	X	X		
		52.192.51.252	ghjap1.axeda.com	X	X	X		
		89.234.8.217	ghuk1.axeda.com	X	X	X		

Device Layer	Network Layer	Enterprise Layer
Built as an application hardened for 24x7 operations in production environments, with automatic restart in event of system or software failure	128-bit SSL encryption	Provides SSL encryption as a default for all communications
128-bit SSL encryption	Utilizes polling server-based communications (to operate within the boundaries set by corporate firewalls)	Requires username and password authentication
Digital certificates	Supports load balancing of network traffic	Supports digital certificates for nonrepudiation with human user and/or devices
Supports auditing of system events locally as well as on the enterprise, allowing local access to audit files		Supports user-level authorization for application functionality (limiting access to device and data views and interaction)
		Supports robust auditing of device and user interactions and system events

Key features and issues addressed by the above implementation of three layer security are summarized below:

The Agent communicates through the firewall using the designated ports. The *Server* is visible to the *Agent* via a documented IP address; the identity of the secure server is known. This obviates any need for the *Agent* to "listen" on a port and consequently be a potential target for unauthorized access. The *Agent* only communicates on the secure tunnel created to the (known) server, thereby eliminating the security risk of communications with an unknown IP address. Customers are welcome to restrict the *Agent's* access to the *Server*. Fully Qualified Domain Names will be available upon request. The *Agent* supports both DHCP and static IP addressing.

The *Agent* is flexible. All of the features described above contribute to flexibility and compatibility in accommodating changing network infrastructures. The *Agent* is not dependent on a static IP address or subnets, and supports corporate network infrastructures that require Internet proxy *Servers*.

Tunnel access is restricted. Once the *Agent* has established a secure tunnel, the connection is visible only to authorized entities. Unauthorized clients and services that try to bind to any free TCP port and protocol cannot use the connection and unauthorized entities cannot use the connection even if they manage to see it.

Security without the cost and inconvenience of a Business to Business VPN. Since the *Agent* is responsible for initiating two-way communication in a manner compliant with the secure computing environment at the customer site, there is no need for a Business to Business virtual private network (VPN). The only requirement is an Internet connection. This is a far less complicated and less costly approach than having to supply, configure and maintain the Business to Business VPN hardware.

Secure Data Transmission. The *Agent* communicates with the *Server* via transmissions that require password authentication to validate the identity of devices exchanging information with the enterprise. All data transmissions are encrypted using 128-bit Secure Socket Layer (SSL) protocol. Digital certificates that validate the recipient before sending data are employed.

Secure *Server* Access. At the enterprise level, VirtualCare® Remote Support allows only users authorized by Bayer HealthCare to log in with username and password authentication. As a further level of security, user log-in profiles control which customers, equipment, and files the user can access, as well as the level of access allowed. All user and system interactions are logged for audit purposes.

Data Protection – Patient data is protected, as Bayer personnel are restricted from accessing such information unless explicitly granted access by the customer during a support incident directly at the site or via remote connection, at which point temporary access is granted. Upon incident resolution, access is terminated by logging off the system. All personnel activity is logged within the system by user logins and all are subject to audit. Internal Bayer quarterly reviews of the audit logs are conducted to verify access, reason, and resolution to further ensure protection of such data.

Bayer

Pharmaceuticals Division

Bayer HealthCare LLC
100 Bayer Boulevard
P.O. Box 915
Whippany, NJ 07981
www.radiologysolutions.bayer.com

Bayer Medical Care Inc.
1 Bayer Drive
Indianola, PA 15051 USA
Contact: +1-800-633-7237 or
Service_Inside_Sales@bayer.com
Customer Service/Orders
+1-800-633-7231
Customer Service Fax
+1-412-767-4120

PP-V-CARE-US-0010 September 2016