VirtualCARE™ Remote Support

Technology and Security for IT Managers

VirtualCARE™
Remote Support

VirtualCARE™ Remote Support

VirtualCARE™ Remote Support allows for advanced remote troubleshooting capabilities and system updates through technology that has been relied on for years in industries like banking and financial services. This document is for Bayer customers, in particular IT managers and administrators, and serves to describe the technology, configuration and security features leveraged to deliver VitualCARE™ Remote Support services.

Overview

The VirtualCARE™ Remote Support infrastructure allows Bayer to remotely service devices and software 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. Their data centers are ISO/IEC 27001:2005 compliant. Designed for high performance and security at every level of its architecture, the solution enables faster response time through remote diagnostics, increased first-time fix rate through diagnosis before dispatch and immediate access to any product software updates that can be delivered remotely. Given these features, VirtualCARE™ Remote Support can facilitate faster overall recovery time and maximise uptime of Bayer products.

Components

VirtualCARE™ Remote Support leverages two major technical components – the *Agent* that is installed on the VirtualCARE™ enabled device or software deployed at the customer site and the *Server* that resides within Bayer's support center. The *Agent*, a software module that runs on the VirtualCARE™ enabled devices, establishes a secure on-demand HTTPS 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* connects to Bayer from behind the safety of the customer's corporate firewall. This connection adheres to all security policies set up by the customer's network administrators. To allow VirtualCARE™ Remote Support connection, the customer's only requirement is to provide outbound internet access for ports 443, 17001, 17002, 80 and 8080.

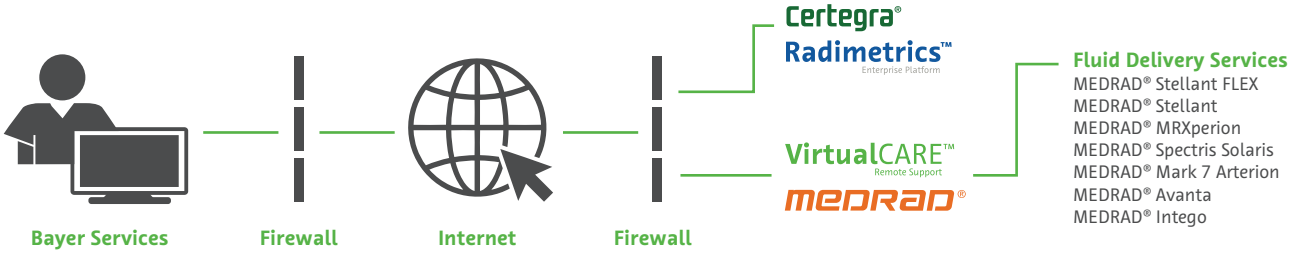
Network Security

Bayer's goal is to support the customer's existing network standards and security practices. A secure three-layer 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, which is built using technology specifically designed for secure, efficient, Intelligent Device Management (IDM) communications. This includes a software design for application security with support for widely used industry standards like TCP/IP, HTTPS, SOAP and XML.

Conclusion

In summary, VirtualCARE™ Remote Support was designed to deliver secure remote connectivity services for Bayer devices and software with the goal of facilitating faster recovery times. To protect against network security risks, VirtualCARE™ leverages the same technology used by leading manufacturers of medical and diagnostic imaging equipment to deliver remote service and monitoring at health care facilities all over the world.

The VirtualCARE™ Remote Support solution does not store or display patient protected health information within the central server.



Radimetrics™ Enterprise Platform

Hostname	Port 443	Port 17001	Port 17002	Port 80	Port 8080
subversion.assembla.com	X			X	
supportserver.radimetrics.com	X			X	X
uksupportserver.radimetrics.com	X			X	X
medrad.axeda.com	X	X	X		
ghsj1.axeda.com	X	X	X		
ghsom1.axeda.com	X	X	X		
Gas-aus.axeda.com	X	X	X		
ghjap1.axeda.com	X	X	X		
ghuk1.axeda.com	X	X	X		

MEDRAD® Injection System Fluid Delivery Devices

Hostname	Port 443	Port 17001	Port 17002
medrad.axeda.com	X	X	X
ghsj1.axeda.com	X	X	X
ghsom1.axeda.com	X	X	X
Gas-aus.axeda.com	X	X	X
ghjap1.axeda.com	X	X	X
ghuk1.axeda.com	X	X	X

Device Layer	Network Layer	Enterprise Layer
Built as an application 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	Utilises 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 authorisation for application functionality (limiting access to device and data views and interaction)
		Supports robust auditing of device and user interactions and system events

The three-layer security architecture that enables VirtualCARE™ Remote Support offers the key features and benefits summarised 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 eliminates the need for the *Agent* to "listen in" on a port and consequently be a potential target for unauthorised 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. If required by the facility's IT protocols, customers may restrict the *Agent's* access to the *Server*. Fully Qualified Domain Names are 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; in addition, it supports corporate infrastructures that require internet proxy *servers*.

Tunnel Access is Restricted. Once the *Agent* has established a secure tunnel, the connection is only visible to authorised entities. Unauthorised clients and services that try to bind to any free TCP port and protocol cannot use the connection. Even if the connection is visible, an unauthorised entity will not be able to access it.

Security comes 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 facility, there is no need for a Business-to-Business Virtual Private Network (VPN). The only requirement is an internet connection. As such, this approach is less complicated and costly than having to supply, configure and maintain the Business-to-Business VPN hardware.

Data transmission is secure. 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. In addition, before data transmissions are processed, the solution requires a digital certificate to validate the recipient.

***Server* access is secure.** At the enterprise level, VirtualCARE™ Remote Support allows only Bayer authorised users to log in with username and password authentication. As an additional 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
Bayer personnel are restricted from accessing certain data unless the customer explicitly grants access permission during a service call, whether in person at the customer facility or via a remote connection. Upon call resolution, Bayer personnel will log out of the system and access will be terminated. All personnel activity is tracked and subject to audit; therefore, you can be assured that your data is protected.

Bayer HealthCare LLC
100 Bayer Boulevard
P.O. Box 915
Whippany, NJ 07981
U.S.A.
Phone: +1-412-767-2400
+1-800-633-7231
Fax: +1-412-767-4120

More information on
radiologysolutions.bayer.com

Manufacturer
Bayer Medical Care Inc.
1 Bayer Drive
Indianola, PA 15051-0780
U.S.A.
Phone: +1-412-767-2400
+1-800-633-7231
Fax: +1-412-767-4120

Authorised Australian Representative
Imaxeon Pty Ltd
Unit 1, 38 – 46 South Street
Rydalmere, NSW 2116
Australia
Phone: +61 2 8845 4999
Fax: +61 2 8845 4998
Customer Service: 1800 633 723

PP-CTD-AU-0003-1 February 2020