VirtualCare Remote Support

Technology and Security White Paper for IT Managers

VirtualCare Remote Support

VirtualCare Remote Support

VirtualCare supports 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 HealthCare 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 HealthCare 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 device to a central *Server* hosted by Axeda'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 Medrad products. Faster response time through remote diagnostics, increased first-time fix rate through diagnosis before dispatch and improved product performance with immediate access to latest product software and enhancements through remote software updates are a few of the benefits made possible by VirtualCare.

VirtualCare is powered by remote connectivity technology from Axeda Corporation, 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.

Components

VirtualCare leverages two major technical components – the *Agent* that is installed on the VirtualCare device deployed at a customer site and the *Server* that resides within Bayer HealthCare's support center. The *Agent*, a software module that runs on the VirtualCare device, establishes a secure on demand HTTPS (port 443) Virtual Private Network (VPN) 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 HealthCare 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 port 443 (https) which is standard on most firewalls.

Network Security

Bayer HealthCare's goal is to support the customer's existing network standards and security practices. The customer's IT department need not make any exceptions to policies or compromise the facility's firewall to enable remote connectivity. This is possible through a three layer security architecture based on Web Services that achieve both transparency and security. 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 Medrad 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.

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* does not require a special port: Typical firewall configurations allow for outbound connections to be initiated securely from behind the firewall over port 443 (HTTPS - Secure Sockets Layer), The *Agent* communicates through the firewall using port 443 and initiates all communication to Bayer HealthCare's *Server*. Therefore, equipment can communicate to the *Server* without revealing its true IP address, in the same way that a web browser accesses a web site. Since all communication is outbound, the facility's network does not need to accept any connections from the outside world or open up ports for remote connectivity. The VirtualCare device will simply not accept connections from any system outside the facility's firewall.

Since the *Server* is visible to the *Agent* via a known IP address, the identity of the secure server is guaranteed. This obviates any need for the *Agent* to "listen" on a port and consequently be a potential target for unauthorized access. The *Agent* only listens to the secure tunnel it has established to the named and trusted Bayer HealthCare *Server* eliminating identity as a potential issue. 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 VPN 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 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 HealthCare

Legal Manufacturer:
Bayer Medical Care Inc.
1 Bayer Drive
Indianola, PA 15051-0780, USA
Telephone: +1 (412) 767-2400
Fax: +1 (412) 767-4120
radiology.bayer.com
healthcare.bayer.com

European Authorized Representative
Bayer Medical Care B.V.
Horsterweg 24
6199 AC Maastricht Airport, The Netherlands
Telephone: +31 (0) 43-3585600
Fax: +31 (0) 43-3656598

CE 0086

VirtualCare INT WP SVC15-300-01 INT