VirtualCARE

Technology and Security White Paper for IT Managers

VirtualCARE

Introduction

VirtualCARE from Bayer in Radiology is designed to deliver secure, reliable remote connectivity and diagnostic services, with the goal of facilitating faster recovery in the event of downtime. VirtualCARE is available for most MEDRAD® injection systems.

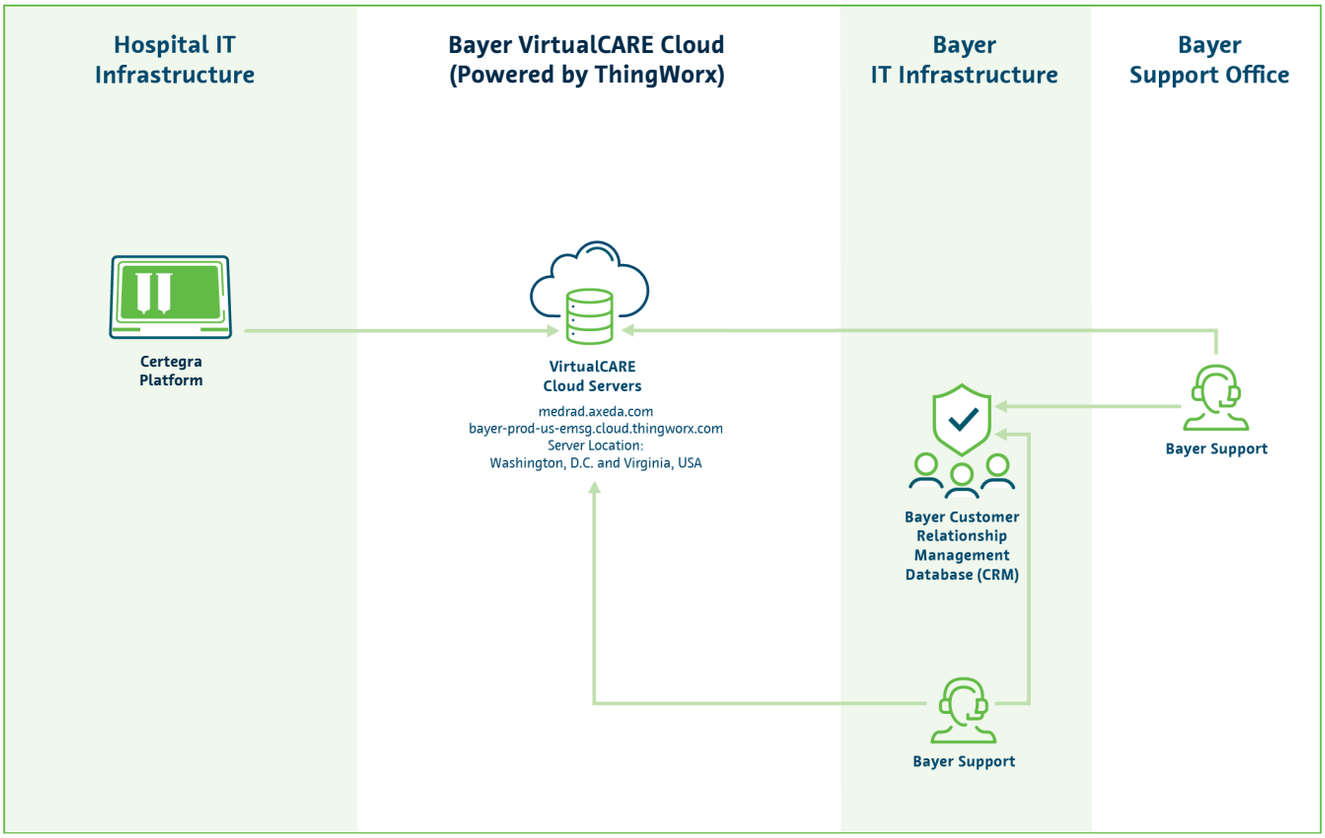
This document serves to describe the VirtualCARE technology, configuration, use and security controls. It also provides the answers to frequently asked questions and outlines the additional resources available to Bayer customers who are implementing VirtualCARE.

Did you know?

- **VirtualCARE is powered by ThingWorx, a remote connectivity technology from PTC, Inc. Bayer relies on ThingWorx to deliver VirtualCARE entitlements to more than 5000 connected customer devices at facilities across the globe.**
- **PTC, which has been partnering with companies for over 30 years to provide IoT, augmented reality, computer-aided design and product lifecycle management technologies, is known for its leading industrial innovation platform. In collaboration with PTC, Bayer has assessed the ThingWorx technology to ensure its compliance with the rigorous Bayer policies that govern data security.**
- **PTC's Cloud Solutions are ISO 27001 audited and certified. PTC Cloud Data Centers are also ISO 27001 certified and SSAE16 SOC Type II Security & Availability Trust Principles audited. In addition, they meet the required security approach for the Federal Risk and Authorization Management Program (FedRAMP).**

Configuration

VirtualCARE enables secure remote connectivity to Bayer devices and software that are installed behind customers' physical, technical and administrative safeguards.



VirtualCARE Usage

There are two main technical components of VirtualCARE: An *agent* installed on a VirtualCARE enabled Bayer device, and the VirtualCARE *cloud servers*.

- VirtualCARE ***cloud servers*** are the back-end management console for user authentication, remote access and diagnostic functions. They also serve as a repository for Bayer device software. The ***cloud servers*** are comprised of a ***main server*** (medrad.axeda.com and bayer-prod-us-emsg.cloud.thingworx.com) and dual, redundant ***remote host servers***.

- Bayer support specialists will authenticate into the ***main server*** using a uniquely assigned user account and complex password, then will select a Bayer product and request remote access. The ***main server*** will route the request to one of two ***remote host servers*** to initiate a remote session.

- The ***agent*** will periodically ping the ***remote hosts*** to detect access requests, triggering a second level of authentication onto a Bayer device or deployed software using a shared Bayer support account.

- If successful, the ***agent*** will create a reverse encrypted tunnel from the Bayer device or installed software to the Bayer support specialist using outbound ports 443, 17001 and 17002. This connection is not dependent on static IP addresses or subnets.

Did you know?

- **Someone must be present at a Bayer device to enable connectivity to the device Operating System or to a MEDRAD® injection system.**

- **Software updates for Bayer devices may be transferred from the VirtualCARE main server, or from a Bayer USB drive by an on-site Bayer Service Engineer.**

- **Bayer will follow the customer's Change Control Process for all troubleshooting, break-fix, update or maintenance activities.**

Security

The VirtualCARE security architecture was built to accommodate existing customer standards and practices by employing security at the device, network and enterprise levels.

Device Level Security

- Hardened software design with automatic restart in the event of system or software failure
- Data transmissions using 128-bit TLS encryption protocol
- Digital certificates utilized to validate recipients before data transmissions are processed
- Auditing enabled to allow VirtualCARE events to be documented at the Bayer device or installed software level and at the VirtualCARE main server

Network Level Security

- Remote host is visible to the agent via static or DHCP reserved IP addresses, eliminating the need for the agent to listen in on a port and consequently be a potential target for unauthorized access
- Agent only communicates via secure tunnel that is reversed from a known support provider, eliminating the security risk of communications with unknown users
- Polling server-based communications (agent 'pings') deliver data files and check for a queue of VirtualCARE scheduled maintenance activities
- VirtualCARE provides no credentials to access the customer's LAN, WAN or non-Bayer devices hosted on the customer's network

Enterprise Level Security

- User access is restricted to trained Bayer support specialists, who access the VirtualCARE application to provide remote support services to entitled customers. Authentication accounts provide specific levels of access, thereby controlling access to Bayer products, actions completed by support staff and actions that can encounter patient records
- Except as noted in documentation for a particular product, no patient protected health information (PHI) is cached, processed or stored outside of a Bayer product that is hosted behind the customer's physical, technical and administrative safeguards

Cybersecurity Threat Response Plan

The ***Radiology Medical Device Cybersecurity*** team maintains a rigorous surveillance and response program for Bayer Products. Bayer monitors external sources including US-CERT and Microsoft® for new cybersecurity vulnerabilities, and then evaluates any new threats for relevance and potential impact on Bayer products. Vulnerabilities requiring remediation are then addressed as part of the Bayer Lifecycle Development and Release program.

Did you know?

- **Bayer employees undergo pre-hire screening and background checks as a condition of employment with Bayer.**
- **Bayer support computers, servers, portable media and networks, as well as Bayer support specialist access to VirtualCARE, are governed by a comprehensive Bayer IT Security Plan.**
- **The Bayer Lifecycle Development and Release program fully supports the requirements of the medical device industry, as specified by the international standard IEC 62304. The Lifecycle Development and Release program aligns with HIPAA and Rev 3 of NIST 800-53 cybersecurity requirements.**

Frequently Asked Questions

Technology

Q: What is VirtualCARE?

A: Bayer in Radiology offers VirtualCARE to deliver remote access for installation, monitoring, support, maintenance and update services to connected customers all over the world. VirtualCARE was designed to improve first-time fix rates through diagnosis before dispatch and offer customers more efficient access to any software updates that can be delivered remotely, for the purpose of facilitating faster recovery in the event of downtime.

Q: How does Bayer enable VirtualCARE?

A: Bayer relies on ThingWorx, a remote access technology from PTC, Inc., to deliver VirtualCARE entitlements. In collaboration with PTC, Bayer has evaluated the ThingWorx application to ensure its compliance with Bayer policies that govern data security and privacy.

Configuration

Q: How is VirtualCARE configured?

A: The VirtualCARE agent will be installed onto Bayer devices. The agent will periodically ping a VirtualCARE remote host to check for access requests or other scheduled maintenance activities. The agent will establish a remote session only after a Bayer user successfully provides two levels of authentication and any additional requirements have been met at the Bayer device level. The agent will reverse an encrypted tunnel from a Bayer support specialist to the Bayer device using a 128-bit TLS encryption protocol.

Q: What action(s) does the customer need to take in order to connect to VirtualCARE?

A: To connect a MEDRAD® injection system to VirtualCARE, the customer needs to provide outbound Internet access for the URLs medrad.axeda.com and bayer-prod-us-emsg.cloud.thingworx.com and for ports 443, 17001 and 17002.

Q: Is customer equipment and software constantly connected to VirtualCARE?

A: Customer devices use the polling method to connect to the VirtualCARE application; as such, the VirtualCARE agent will 'ping' the remote host every 30 seconds.

Security

Q: How is the VirtualCARE security architecture designed?

A: The VirtualCARE application employs security features at the device, network and enterprise levels.

Q: How does the VirtualCARE security architecture address data transmission security?

A: All data transmissions occur within an encrypted tunnel established via 128-bit TLS encryption protocol. The agent communicates with a server or support provider via transmissions that require two levels of user authentication to validate a remote support session. Before data transmissions are processed, VirtualCARE requires a digital certificate to validate the recipient.

Q: How does the VirtualCARE security architecture address enterprise security?

A: VirtualCARE allows only trained, US and Canadian based Bayer support specialists to establish remote support sessions. Sessions are logged at the VirtualCARE remote host and installed Bayer device or software. In addition, sessions are documented in the Bayer CRM database. VirtualCARE does not provide credentials to access the customer's LAN, WAN or non-Bayer devices or software.

Q: Does the VirtualCARE application store PHI?

A: Except as noted in documentation for a particular product, no PHI is cached, processed or stored outside of a Bayer product that is hosted behind the customer's physical, technical and administrative safeguards.

Other

Q: My facility requires documentation to confirm that VirtualCARE adheres to its security policies. Can Bayer provide that documentation?

A: Yes, upon request, Bayer will make every effort to work with customers to complete comprehensive cybersecurity reviews in line with hospital policies.

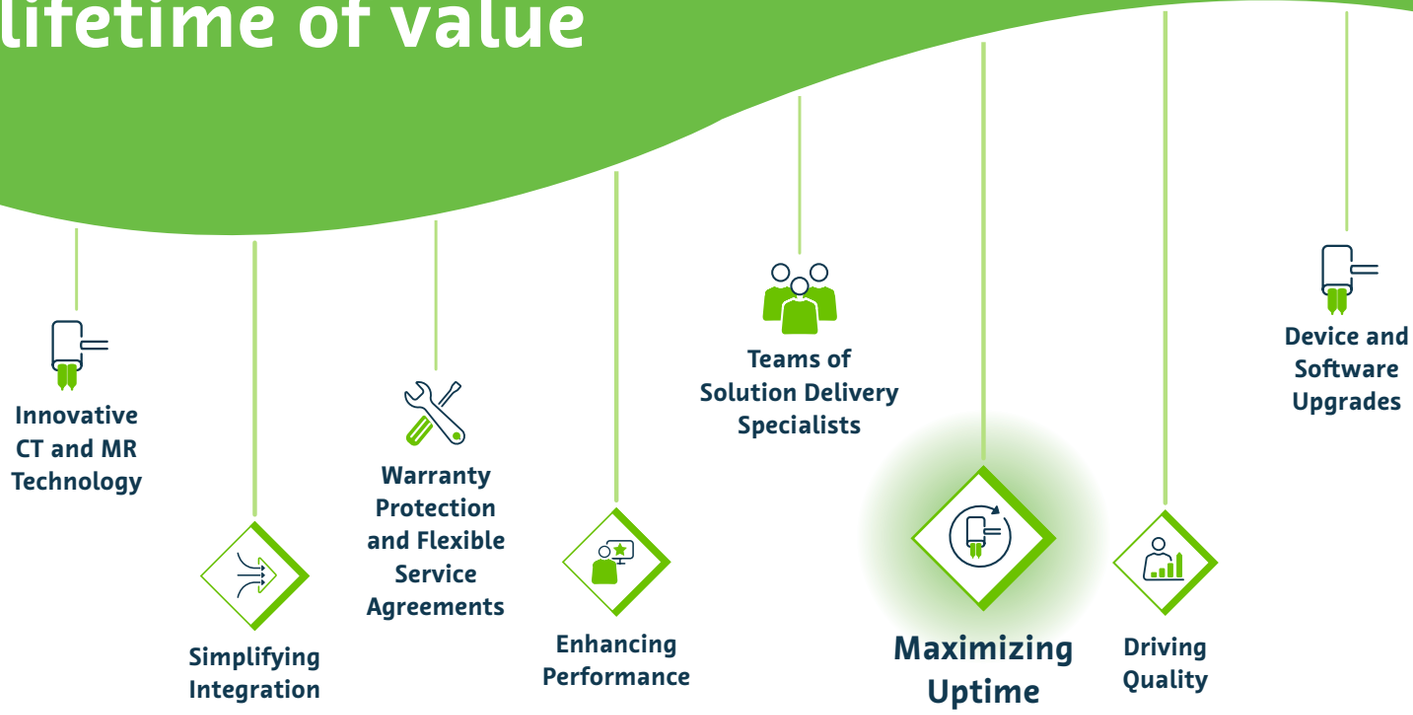
Q: How does Bayer monitor and assess cybersecurity threats?

A: The Radiology Medical Device Cybersecurity team maintains a rigorous surveillance and response program for Bayer devices and software. The Radiology Services Information Technology Advisory page provides ongoing updates related to cybersecurity surveillance and response at: https://www.radiologysolutions.bayer.com/information-technology-advisory.

Additional Resources:

Bayer Technical Assistance Centers for Device or Software Support
radiologycanadianservice@bayer.com

At every step, Bayer is there with Services that deliver a lifetime of value



2920 Matheson Blvd East
Mississauga ON L4W 5R6
Phone: (800) 268-1432
Fax: (800) 567-1710

PP-PF-RAD-CA-0724-2 August 2025