The Technology behind VirtualCARE

At Bayer, we envision a future where every power injected procedure is delivered from well connected hardware, software, and services. When technology is securely and seamlessly connected through VirtualCARE, processes can be streamlined, data can drive better management decisions, and your team is able to focus on what matters most—the patient.

VirtualCARE
Remote Connectivity White Paper

Introduction

Bayer solutions are powered by connectivity, which starts with remote connection.

Remote connection can be enabled on any Bayer SMART injector, including MEDRAD® Centargo, MEDRAD® Stellant and MEDRAD® MRXperion. A consistent connection to Bayer's remote access server is essential for installing cybersecurity patches, activating remote diagnostics and technical support, and managing subscriptions to licensed software and services throughout the injector's lifecycle.

This document outlines the technology, configuration, use, and security controls for remote connectivity of Bayer SMART injectors and serves as a resource for frequently asked questions and customer support during implementation.

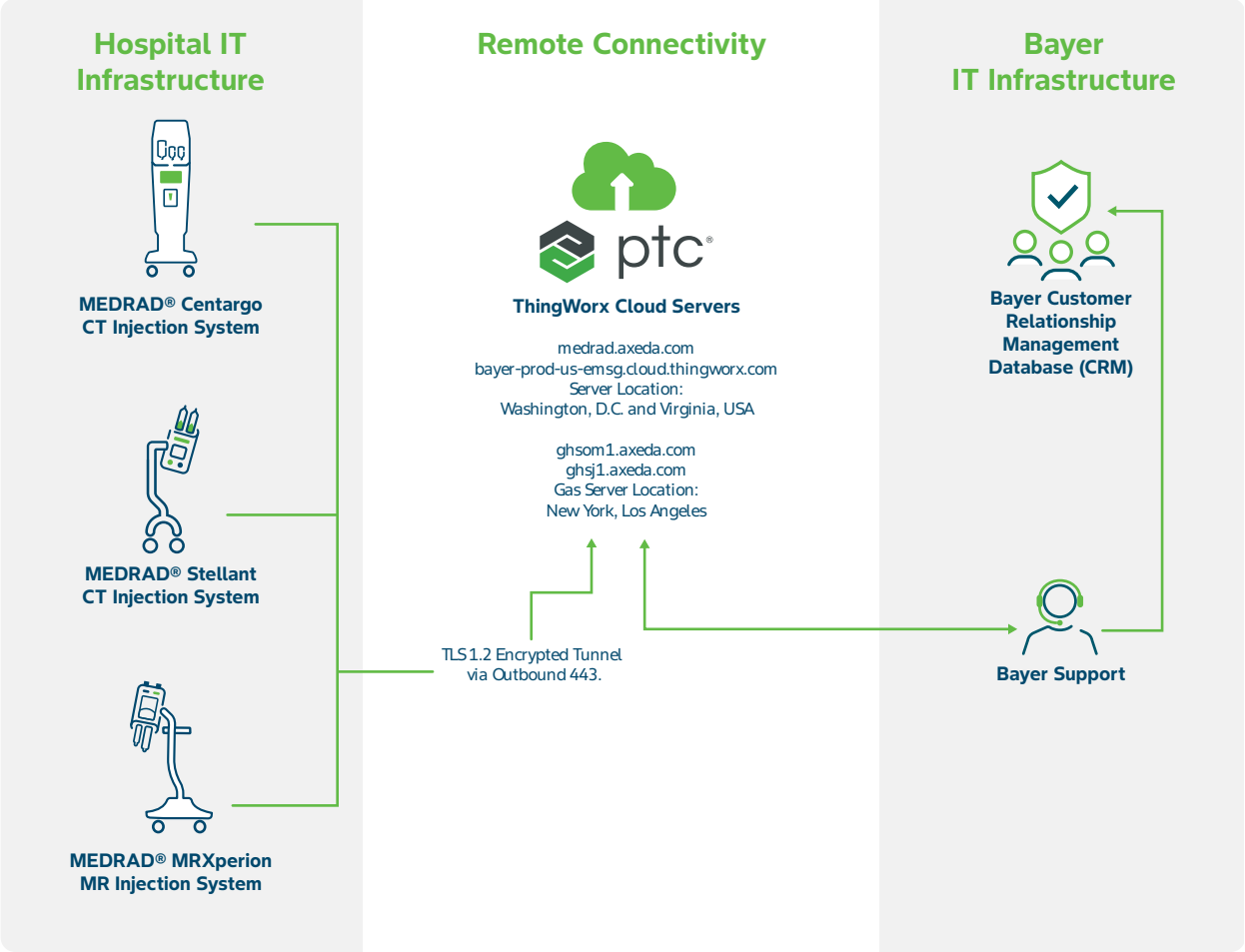
Connectivity for Bayer SMART Injectors

Did you know?

- Bayer delivers remote connectivity for SMART injectors through ThingWorx, which is remote access server technology from PTC, Inc.
- 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.

Configuration

Bayer's technology enables secure remote connectivity to SMART injectors installed behind physical, technical and administrative safeguards at the customer facility.



Server Name	Fully Qualified Domain Name (FQDN)	IP	Location	Port
Production	medrad.axeda.com	13.82.188.8	Virginia	443
Production	bayer-prod-us-emsg.cloud.thingworx.com	13.82.188.8	Virginia	443
Global Access Server	gas-ghsom1.cloud.thingworx.com	54.80.26.190	Virginia	443
Global Access Server	ghsom1.axeda.com	209.202.157.179	New York	443
Global Access Server	ghsj1.axeda.com	52.8.82.253	Los Angeles	443

Technical Considerations

There are two main technical components of Bayer's remote connectivity solution: An agent installed on a connected SMART injector and the ThingWorx cloud servers.

- ThingWorx 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 and software updates and patches. The ***cloud servers*** are comprised of a main server (medrad.axeda.com and bayer-prod-us-emsg.cloud.thingworx.com) and dual, redundant Global Access Servers (GAS), which are located in New Jersey and California, USA.

- Bayer support specialists authenticate into the main server using uniquely assigned user accounts and Single Sign-On (SSO) with multi-factor authentication (MFA) to ensure secure access. In alignment with the principle of least privilege, users are granted access only to the systems and data necessary to perform their specific support functions. Once authenticated, the specialist selects the relevant Bayer product and submits a remote access request. The main server then securely routes this request to one of the designated Global Access Servers (GAS) servers listed above.

- The ***agent*** will periodically ping the ***remote hosts*** to detect access requests, triggering a second level of authentication onto a Bayer SMART injector using a Bayer support account.

- The agent periodically pings remote hosts to detect access requests, triggering second-level authentication on the Bayer SMART injector. If successful, it establishes a reverse encrypted tunnel to the Bayer support specialist using outbound port 443. OS-level access requires physical presence and approval at the SMART injector to enable remote connectivity.

Did you know?

- Someone must be present at the Bayer SMART injector to enable remote connectivity to the device operating system.

- Software updates and patches for Bayer SMART injectors may be transferred from The ThingWorx main server.

- Where supported, cybersecurity patches may be deployed automatically through Bayer's secure remote connectivity platform.

Security

The security architecture underlying Bayer's remote connectivity solution 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 1.2 encryption protocol
- Digital certificates utilized to validate recipients before data transmissions are processed
- Auditing enabled to allow remote service events to be documented at the Bayer device or and at the ThingWorx 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 the injector to ThingWorx eliminating the security risk of communications with unknown users
- Polling server-based communications (agent 'pings') deliver data files and check for a queue of scheduled maintenance activities
- Bayer's remote connectivity solution 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 remote access server 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
- No patient protected health information (PHI) or personally identifiable information (PII) is cached, processed or stored outside of a Bayer SMART injector 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 SMART injectors and software. 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.

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.**

Did you know?

- Bayer employees undergo pre-hire screening and background checks as a condition of employment with Bayer.
- Bayer supported computers, servers, portable media, and networks, as well as Bayer support specialist access to remote access server, 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 Food and Drug Administration (FDA) in 21 CFR 820 Quality System Regulation and the international standard IEC 62304. The Lifecycle Development and Release program aligns with HIPAA and Rev 3 of NIST 800-53 cybersecurity requirements.

Additional Resources:

- **Device Support: TAC@Bayer.com**
- **Connectivity Support: TACvirtualcare@Bayer.com**
- **CyberSecurity Support: TAC.cybersecurity@Bayer.com**

Frequently Asked Questions

Technology

Q: Why does Bayer offer remote connectivity?

A: Bayer solutions are powered by connectivity, which starts with remote connection. Remote connection can be enabled on any Bayer SMART injector, including MEDRAD® Centargo, MEDRAD® Stellant and MEDRAD® MRXperion. A consistent connection to Bayer's remote access server is essential for installing cybersecurity patches, activating remote diagnostics and technical support, and managing subscriptions to licensed software and services throughout the injector's lifecycle.

Q: How does Bayer enable remote connectivity to SMART injectors and software?

A: Bayer relies on ThingWorx, a remote access technology from PTC, Inc., to enable remote connectivity and deliver remote diagnostics and technical support services to entitled customers. 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 a remote connection configured?

A: The ThingWorx agent is pre-installed on all Bayer SMART injectors. The agent will ping the main ThingWorx server every 30 seconds 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 SMART injector level. The agent will reverse an encrypted tunnel from a Bayer support specialist to the Bayer SMART injector using a 128-bit TLS 1.2 encryption protocol.

Q: What action(s) does the customer need to take in order to establish a remote connection?

A: To connect a Bayer SMART injector, the customer only needs to provide outbound access on port 443 for the following URLs: medrad.axeda.com; bayer-prod-us-emsg.cloud; thingworx.com; ghsom1.axeda.com; and ghsj1.axeda.com.

Q: How is customer equipment and software constantly connected to ThingWorx?

A: Bayer SMART injectors use a polling method to connect to Bayer's main ThingWorx server. As such, the ThingWorx agent on the device will ping the main server every 30 seconds.

Security

Q: How is Bayer's remote connectivity security architecture designed?

A: The remote server employs security features at the device, network and enterprise levels.

Q: How does Bayer's remote connectivity security architecture address data transmission security?

A: All data transmissions occur within an encrypted tunnel established via 128-bit TLS 1.2 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, Bayer's remote connectivity requires a digital certificate to validate the recipient.

Q: How does the Bayer's remote connectivity security architecture address enterprise security?

A: Bayer support specialists authenticate into the main server using uniquely assigned user accounts and Single Sign-On (SSO) with multi-factor authentication (MFA) to ensure secure access. In alignment with the principle of least privilege, users are granted access only to the systems and data necessary to perform their specific support functions. Once authenticated, the specialist selects the relevant Bayer product and submits a remote access request. The main server then securely routes this request to one of the designated GAS servers listed above.

Q: Does the ThingWorx remote connectivity application store PHI?

A: No patient data is cached, processed or stored outside of a Bayer SMART injector that is hosted behind the customer's physical, technical and administrative safeguards. *continued on following page*

Other

Q: My facility requires documentation to confirm that Bayer's remote connectivity solution 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. Cybersecurity reviews can be sent to TAC.cybersecurity@bayer.com for review and completion.

Q: How does Bayer monitor and assess cybersecurity threats?

A: Bayer follows FDA Post-Market guidance for vulnerability reporting and patching, which requires 30 days to communicate after discovery and 60 days to patch, relative to an uncontrolled patient safety risk. This timing is due to the fact that, per our medical device development process, any required patches must go through a rigorous Design, Verification, Validation and Release process.

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**.

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

More information on
radiology.bayer.ca

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

PP-PF-RAD-CA-0989-1 March 2026

Our dedicated Bayer Cybersecurity Team and subject matter experts in healthcare IT are available to answer your questions and support site specific needs.

Click here to contact our dedicated Bayer Cybersecurity Team ›