VirtualCARE

La technologie derrière VirtualCARE

Chez Bayer, nous envisageons un avenir où chaque injection automatique s'appuiera sur un équipement, un logiciel et des services connectés. Lorsque les technologies sont connectées de manière sécurisée et transparente par VirtualCARE, les processus peuvent être simplifiés, les données permettent de prendre de meilleures décisions de traitement, et votre équipe peut se concentrer sur ce qui compte le plus : le patient.

VirtualCARE
Livre blanc sur la connectivité à distance

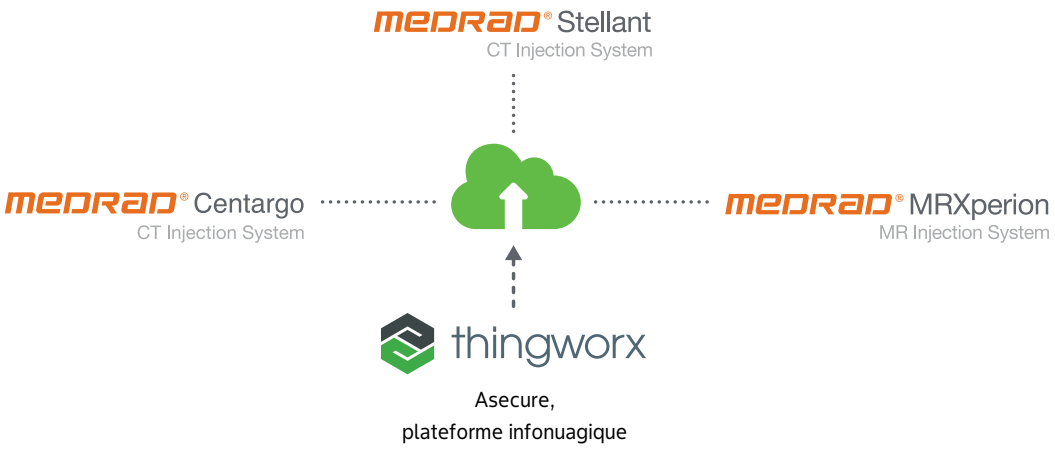
Introduction

Les solutions de Bayer s'appuient sur la connectivité, qui commence par la connexion à distance

La connexion à distance peut être activée sur n'importe quel injecteur SMART de Bayer, y compris MEDRAD® Centargo, MEDRAD® Stellant et MEDRAD® MRXperion. Une connexion stable au serveur d'accès à distance de Bayer est indispensable pour installer les correctifs de cybersécurité, activer les diagnostics à distance et le soutien technique, ainsi que pour gérer les abonnements aux logiciels sous licence et aux services tout au long du cycle de vie de l'injecteur.

Ce document présente la technologie, la configuration, l'utilisation et les mesures de sécurité relatives à la connectivité à distance des injecteurs SMART de Bayer; il sert aussi de référence pour les questions fréquentes et le soutien à la clientèle lors de la mise en œuvre.

Connectivité pour les injecteurs SMART de Bayer

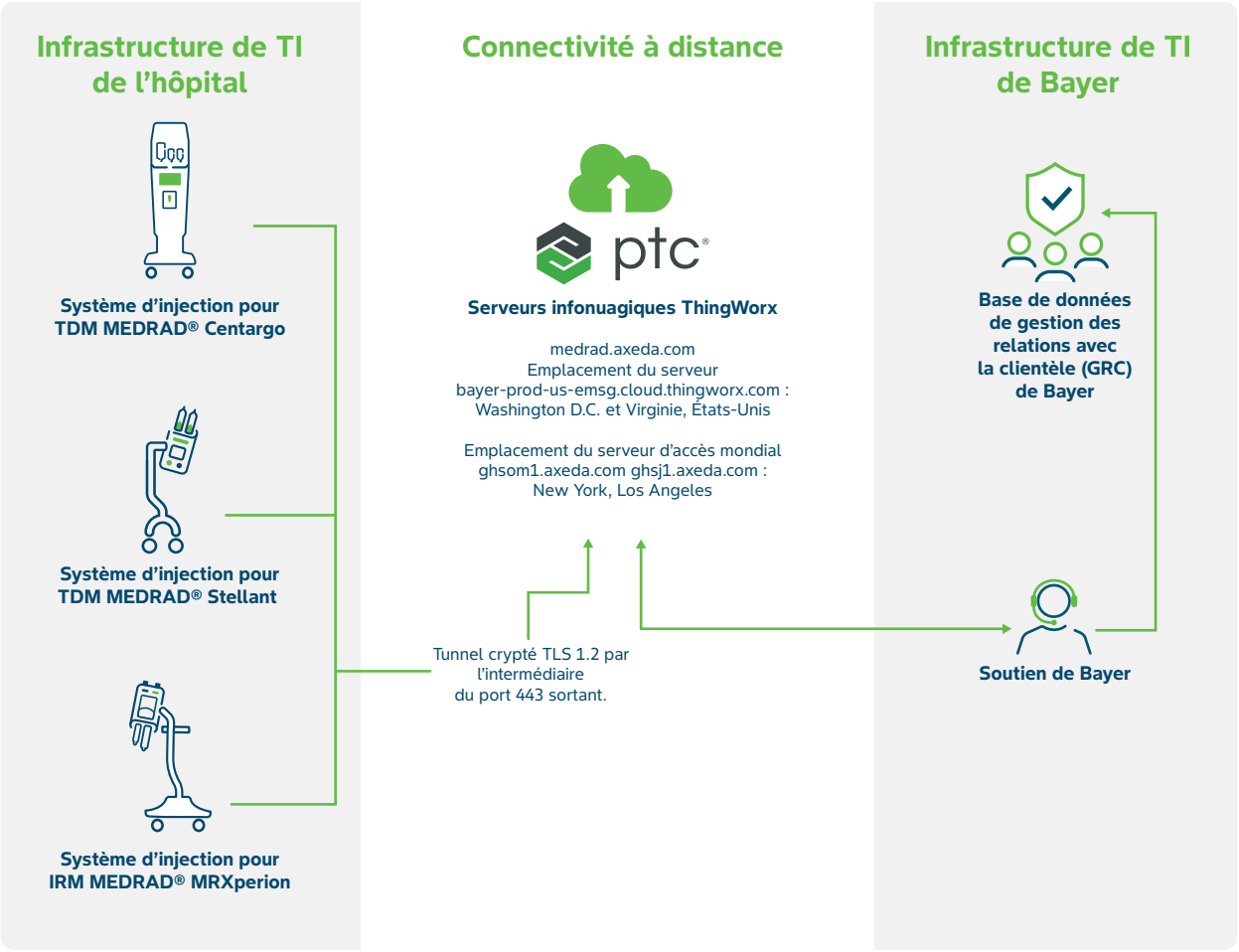


Le saviez-vous?

- Bayer assure la connectivité à distance des injecteurs SMART grâce à ThingWorx, une technologie de serveur d'accès à distance conçue par PTC, Inc.
- La société PTC, partenaire des entreprises depuis plus de 30 ans en vue d'offrir des technologies liées à l'Internet des objets, à la réalité augmentée, à la conception assistée par ordinateur et à la gestion du cycle de vie des produits, est reconnue pour sa plateforme d'innovation industrielle d'avant-garde. En collaboration avec PTC, Bayer a évalué l'application ThingWorx pour veiller à ce qu'elle respecte ses politiques rigoureuses en matière de sécurité des données.
- Les solutions infonuagiques de PTC sont contrôlées et certifiées selon la norme ISO 27001. Les centres de données infonuagiques PTC sont également certifiés ISO 27001 et les principes de confiance de sécurité et de disponibilité de type II du SOC SSAE16 sont vérifiés.

Configuration

La technologie de Bayer permet une connexion à distance sécurisée aux injecteurs SMART installés dans l'établissement du client et protégés par ses mesures de protection physiques, techniques et administratives.



Server Name	Fully Qualified Domain Name (FQDN)	IP	Location	Port
Production	medrad.axeda.com	13.82.188.8	Virginie	443
Production	bayer-prod-us-emsg.cloud.thingworx.com	13.82.188.8	Virginie	443
Serveur d'accès mondial	gas-ghsom1.cloud.thingworx.com	54.80.26.190	Virginie	443
Serveur d'accès mondial	ghsom1.axeda.com	209.202.157.179	New York	443
Serveur d'accès mondial	ghsj1.axeda.com	52.8.82.253	Los Angeles	443

Aspects techniques

La solution de connectivité à distance de Bayer repose sur deux composantes techniques principales : un agent installé sur un injecteur SMART connecté et les serveurs infonuagiques ThingWorx.

- Les serveurs infonuagiques ThingWorx constituent la console de gestion d'arrière-plan pour l'authentification des utilisateurs, l'accès à distance et les fonctions de diagnostic. Ils servent également de référentiel pour les mises à jour et correctifs de logiciels et d'appareils de Bayer. Les serveurs infonuagiques se composent d'un serveur principal (medrad.axeda.com et bayer-prod-us-emsg.cloud.thingworx.com) et de deux serveurs d'accès mondial redondants, situés respectivement au New Jersey et en Californie, aux États-Unis.

- Chaque spécialiste du soutien de Bayer se connecte au serveur principal à l'aide de son compte d'utilisateur et d'une authentification unique associée à une authentification multifactorielle afin de garantir un accès sécurisé. Conformément au principe de « droit d'accès minimal », les utilisateurs ne se voient accorder l'accès qu'aux systèmes et aux données nécessaires à l'exercice de leurs fonctions spécifiques au soutien. Une fois authentifié, le spécialiste sélectionne le produit de Bayer concerné et envoie une demande d'accès à distance. Le serveur principal achemine ensuite cette requête de manière sécurisée vers l'un des serveurs d'accès mondial désignés mentionnés ci-dessus.

- L'agent sondera périodiquement les serveurs hôtes à distance pour détecter les demandes d'accès, déclenchant un second niveau d'authentification sur un injecteur SMART de Bayer à l'aide d'un compte de soutien de Bayer.

- L'agent sonde périodiquement les hôtes distants afin de détecter les demandes d'accès, ce qui déclenche une authentification de deuxième niveau sur l'injecteur SMART de Bayer. En cas de réussite du processus, il établit un tunnel crypté inverse vers le spécialiste du soutien de Bayer par le port sortant 443. L'accès au niveau du système d'exploitation nécessite une présence physique et une autorisation au niveau de l'injecteur SMART pour activer la connectivité à distance.

Did you know?

- Une personne doit se trouver près de l'injecteur SMART de Bayer pour permettre la connexion à distance au système d'exploitation de l'appareil.

- Les mises à jour logicielles et les correctifs destinés aux injecteurs SMART de Bayer peuvent être téléchargés à partir du serveur principal de ThingWorx.

- Lorsque cela est pris en charge, les correctifs de cybersécurité peuvent être déployés automatiquement par la plateforme de connectivité à distance sécurisée de Bayer.

Security

L'architecture de sécurité sous-jacente de la solution de connectivité à distance de Bayer a été conçue pour répondre aux normes et aux pratiques des clients existants en utilisant la sécurité à l'échelle de l'appareil, du réseau et de l'entreprise.

Sécurité au niveau des dispositifs

- Conception de logiciel renforcée permettant un redémarrage automatique dans le cas d'une défaillance du système ou du logiciel.
- Transmissions de données au moyen du protocole de chiffrement TLS 1.2 de 128 bits.
- Certificats numériques utilisés pour valider les destinataires avant le traitement des transmissions de données.
- Vérification activée pour permettre la documentation des activités de service à distance au niveau de l'appareil de Bayer ou du serveur principal de ThingWorx.

Sécurité au niveau du réseau

- Le serveur hôte distant est visible par l'agent au moyen d'adresses IP statiques ou réservées au protocole DHCP, ce qui élimine la nécessité pour l'agent d'écouter sur un port et, par conséquent, d'être une cible potentielle pour un accès non autorisé.
- L'agent communique uniquement au moyen d'un tunnel sécurisé inversé de l'injecteur à ThingWorx, ce qui élimine le risque de sécurité lié aux communications avec des utilisateurs inconnus.
- Les sondages du serveur par l'agent permettent de fournir des fichiers de données et de rechercher une file d'attente des activités de maintenance prévues.
- La solution de connectivité à distance de Bayer ne fournit aucune information d'identification pour accéder aux dispositifs en réseau local, en réseau étendu ou autres que ceux de Bayer hébergés sur le réseau du client.

Sécurité au niveau de l'entreprise

- L'accès utilisateur est limité aux spécialistes du soutien formés par Bayer qui accèdent au serveur d'accès à distance pour offrir des services de soutien à distance aux clients qui y ont droit. Les comptes d'authentification accordent des niveaux d'accès spécifiques, ce qui permet de contrôler l'accès aux produits de Bayer, les mesures prises par le personnel de soutien et les mesures qui peuvent être prises pour obtenir les dossiers des patients.
- Aucun renseignement médical protégé ni aucun renseignement personnel n'est mis en cache, traité ou conservé en dehors d'un injecteur SMART de Bayer, lequel est protégé au moyen des mesures de sécurité physiques, techniques et administratives mises en place par le client.

Plan d'intervention contre les menaces de cybersécurité

L'équipe de ***cybersécurité des dispositifs médicaux de radiologie*** maintient un programme rigoureux de surveillance et d'intervention pour les injecteurs SMART et logiciels de Bayer. Bayer surveille les sources externes, notamment US-CERT et Microsoft®, pour détecter les nouvelles vulnérabilités en matière de cybersécurité, puis évalue la pertinence de toute nouvelle menace et son incidence éventuelle sur les produits de Bayer. Les vulnérabilités exigeant des mesures correctives sont ensuite traitées dans le cadre du programme de développement et de gestion des versions du cycle de vie de Bayer.

La page d'avis sur les technologies de l'information des services de radiologie, accessible au **https://www.radiologysolutions.bayer.com/** information-technology-advisory, propose des mises à jour continues concernant la surveillance et les interventions en matière de cybersécurité.

Le saviez-vous?

- Les employés de Bayer sont soumis à un contrôle préalable à l'embauche et à une vérification des antécédents comme condition d'emploi chez Bayer.
- Les ordinateurs, serveurs, dispositifs portables et réseaux du service de soutien de Bayer, ainsi que l'accès des spécialistes du soutien de Bayer au serveur d'accès à distance, sont régis par un plan de sécurité des TI complet de Bayer.
- Le programme de développement et de gestion des versions du cycle de vie de Bayer répond pleinement aux exigences du secteur des dispositifs médicaux, telles que définies par la Food and Drug Administration (FDA) dans le règlement sur les systèmes qualité 21 CFR 820 et la norme internationale CEI 62304. Le programme de développement et de gestion des versions du cycle de vie est conforme aux exigences de la HIPAA et de la Rév. 3 de la NIST 800-53 en matière de cybersécurité.

Ressources supplémentaires :

- **Soutien relatif aux appareils : TAC@Bayer.com**
- **Soutien relatif à la connectivité : TACvirtualcare@Bayer.com**
- **Soutien relatif à la cybersécurité : TAC.cybersecurity@Bayer.com**

Foire aux questions

Technologie

Q : Pourquoi Bayer offre-t-elle une connectivité à distance?

R : Les solutions de Bayer s'appuient sur la connectivité, qui commence par la connexion à distance. La connexion à distance peut être activée sur n'importe quel injecteur SMART de Bayer, y compris MEDRAD® Centargo, MEDRAD® Stellant et MEDRAD® MRXperion. Une connexion stable au serveur d'accès à distance de Bayer est indispensable pour installer les correctifs de cybersécurité, activer les diagnostics à distance, bénéficier d'un soutien technique et gérer les abonnements aux logiciels sous licence et aux services tout au long du cycle de vie de l'injecteur.

Q : Comment Bayer permet-elle la connectivité à distance aux injecteurs SMART et aux logiciels?

R : Bayer s'appuie sur ThingWorx, une technologie d'accès à distance conçue par PTC, Inc., pour permettre la connectivité à distance et offrir des services de diagnostic et de soutien technique à distance aux clients qui y ont droit. En collaboration avec PTC, Bayer a évalué l'application ThingWorx pour veiller à ce qu'elle respecte les politiques de Bayer en matière de sécurité et de protection des données.

Configuration

Q : Comment configure-t-on une connexion à distance?

R : L'agent ThingWorx est préinstallé sur tous les injecteurs SMART de Bayer. Il sondera le serveur ThingWorx principal toutes les 30 secondes afin de vérifier s'il y a des demandes d'accès ou d'autres opérations de maintenance programmées. L'agent n'établira une séance à distance que lorsqu'un utilisateur de Bayer aura réussi à fournir deux niveaux d'authentification et que toute autre exigence aura été satisfaite au niveau de l'injecteur SMART de Bayer. L'agent inversera un tunnel chiffré entre un spécialiste du soutien de Bayer et l'injecteur SMART de Bayer au moyen d'un protocole de chiffrement TLS 1.2 de 128 bits.

Q : Quelles mesures le client doit-il prendre pour établir une connexion à distance?

R : Pour connecter un injecteur SMART de Bayer, il suffit au client d'autoriser l'accès sortant sur le port 443 pour les URL suivantes : medrad.axeda.com, bayer-prod-us-emsg.cloud, thingworx.com, ghsom1.axeda.com et ghsj1.axeda.com.

Q : Comment les équipements et logiciels des clients sont-ils constamment connectés à ThingWorx?

R : Les injecteurs SMART de Bayer utilisent une méthode de sondage pour se connecter au serveur ThingWorx principal de Bayer. Ainsi, l'agent ThingWorx installé sur l'appareil sondera le serveur principal toutes les 30 secondes.

Sécurité

Q : Comment l'architecture de sécurité de la connectivité à distance de Bayer est-elle conçue?

R : Le serveur à distance utilise des fonctions de sécurité à l'échelle de l'appareil, du réseau et de l'entreprise.

Q : Comment l'architecture de sécurité de connectivité à distance de Bayer aborde-t-elle la sécurité de la transmission des données?

R : Toutes les transmissions de données se font dans un tunnel chiffré établi au moyen d'un protocole de chiffrement TLS 1.2 de 128 bits. L'agent communique avec un serveur ou un fournisseur de soutien au moyen de transmissions qui exigent deux niveaux d'authentification de l'utilisateur pour valider une séance de soutien à distance. Avant le traitement des transmissions de données, la connectivité à distance de Bayer exige un certificat numérique pour valider le destinataire.

Q : Comment l'architecture de sécurité de connectivité à distance de Bayer aborde-t-elle la sécurité de l'entreprise?

R : Chaque spécialiste du soutien de Bayer se connecte au serveur principal à l'aide de son compte d'utilisateur et d'une authentification unique associée à une authentification multifactorielle afin de garantir un accès sécurisé. Conformément au principe du « droit d'accès minimal », les utilisateurs ne se voient accorder l'accès qu'aux systèmes et aux données nécessaires à l'exercice de leurs fonctions spécifiques au soutien. Une fois authentifié, le spécialiste sélectionne le produit Bayer concerné et envoie une demande d'accès à distance. Le serveur principal achemine ensuite cette requête de manière sécurisée vers l'un des serveurs d'accès mondial désignés mentionnés plus haut.

Q : L'application de connectivité à distance ThingWorx conserve-t-elle des renseignements médicaux protégés?

R : Aucun renseignement sur les patients n'est mis en cache, traité ou conservé en dehors d'un injecteur SMART de Bayer, lequel est hébergé dans le respect des mesures de sécurité physiques, techniques et administratives mises en place par le client.

Autre

Q : Mon établissement exige des documents attestant que la solution de connectivité à distance de Bayer respecte ses politiques de sécurité. Bayer peut-elle fournir ces documents?

R : Oui, sur demande, Bayer fera tout son possible pour collaborer avec ses clients afin de réaliser des examens complets de cybersécurité, conformément aux politiques des hôpitaux. Les rapports sur la cybersécurité peuvent être envoyés à TAC.cybersecurity@bayer.com en vue de leur examen et de leur finalisation.

Q : Comment Bayer surveille-t-elle et évalue-t-elle les menaces de cybersécurité?

R : Bayer suit les recommandations de la FDA relatives à la déclaration des vulnérabilités et à l'application de correctifs après la mise sur le marché, qui prévoient un délai de 30 jours pour la déclaration après la découverte et de 60 jours pour l'application du correctif, en cas de risque non maîtrisé pour la sécurité des patients. Ce délai s'explique par le fait que, conformément à notre processus de développement des dispositifs médicaux, tout correctif nécessaire doit suivre un processus rigoureux de conception, de vérification, de validation et de mise en service.

La page d'avis sur les technologies de l'information des services de radiologie, accessible au **https://www.radiologysolutions.bayer.com/ information-technology-advisory**, propose des mises à jour continues concernant la surveillance et les interventions en matière de cybersécurité.

Bayer Inc.
2920 Matheson Blvd. East,
Mississauga (Ontario)
L4W 5R6
Tél. : 1-800-268-1432
Téléc. : 1-800-567-1710

Pour en savoir plus, visitez le site
www.radiology.bayer.ca/fr

Fabricant
Bayer Medical Care Inc.
1 Bayer Drive
Indianola, PA 15051-0780
États-Unis
Tél. : 1-412-767-2400
1-800-633-7231
Téléc. : 1-412-767-4120

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

Notre équipe de cybersécurité de Bayer attitrée, ainsi que nos experts en TI de la santé, sont à votre disposition pour répondre à vos questions et vous aider à répondre aux besoins particuliers de votre établissement.

Cliquez ici pour communiquer avec notre équipe de cybersécurité de Bayer attitrée