VirtualCARE

Livre blanc sur la technologie et la sécurité à l'intention des gestionnaires de TI

VirtualCARE

Introduction

VirtualCARE de la Radiologie de Bayer est conçu pour offrir une connectivité et des services de diagnostic à distance sûrs et fiables, dans le but de permettre une reprise plus rapide en cas de panne. VirtualCARE est offert pour la plupart des systèmes d'injection MEDRAD®.

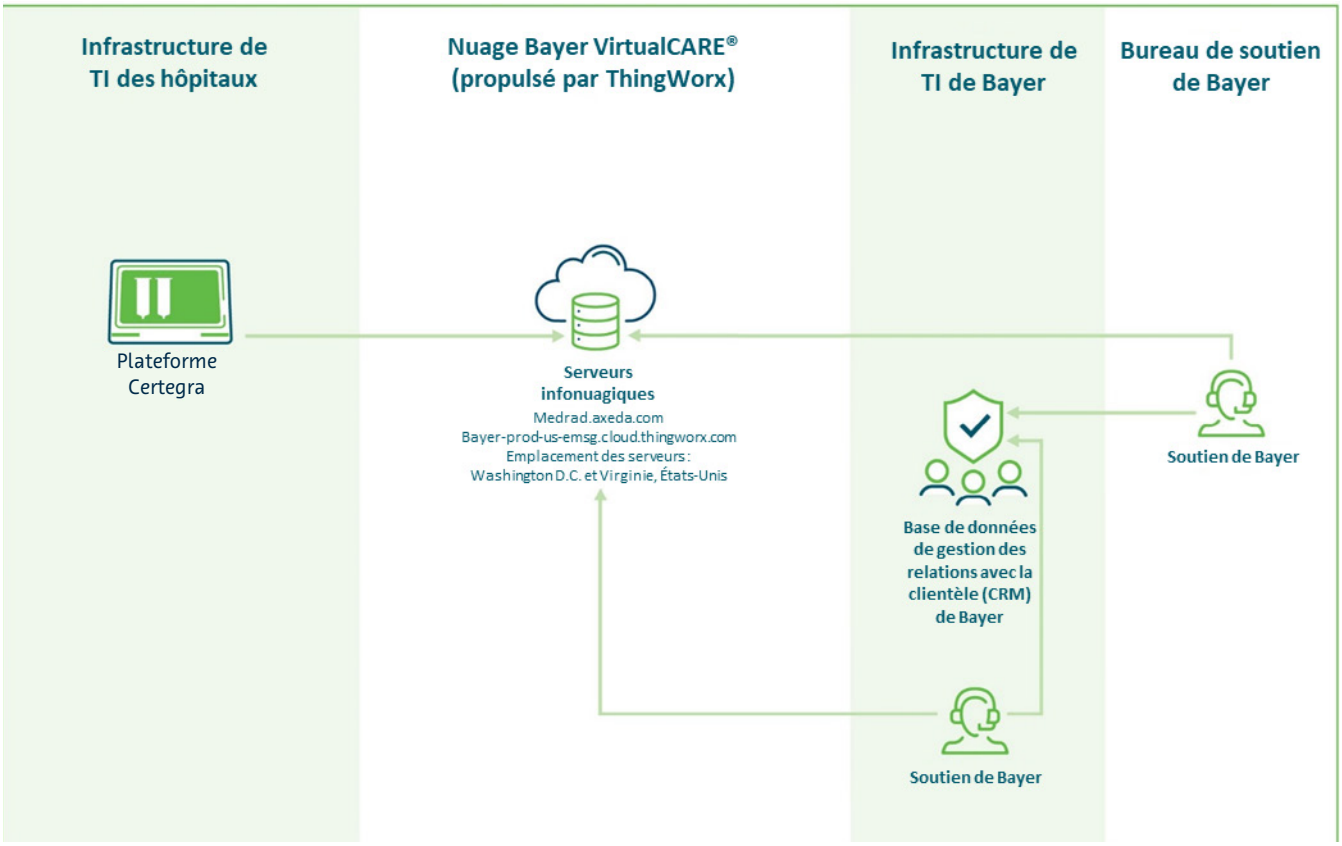
Ce document a pour objectif de décrire la technologie, la configuration, l'utilisation et les contrôles de sécurité de VirtualCARE. Il répond également aux questions fréquemment posées et précise les ressources supplémentaires mises à la disposition des clients de Bayer qui mettent en œuvre VirtualCARE.

Le saviez-vous?

- **VirtualCARE est optimisé par ThingWorx, une technologie de connectivité à distance de PTC, Inc. Bayer s'appuie sur ThingWorx pour fournir des droits VirtualCARE à plus de 5 000 appareils clients situés dans des installations du monde entier..**
- **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 examiné l'application ThingWorx afin de s'assurer de sa conformité avec les politiques rigoureuses de Bayer qui régissent la 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. De plus, ils satisfont à l'approche de sécurité requise par le Federal Risk and Authorization Management Program (FedRAMP).**

Configuration

VirtualCARE permet une connectivité à distance sécurisée avec les appareils et les logiciels de Bayer installés et protégés par les mesures de protection physiques, techniques et administratives des clients.



Utilisation de VirtualCARE

Il existe deux principaux éléments techniques de VirtualCARE : un *agent* installé sur un dispositif de Bayer utilisé pour VirtualCARE et les *serveurs infonuagiques* de VirtualCARE.

- Les ***serveurs infonuagiques*** VirtualCARE 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 logiciels des appareils de Bayer. Les ***serveurs infonuagiques*** sont composés d'***un serveur principal*** (medrad.axeda.com et bayer-prod-us-emsg.cloud.thingworx.com) et de deux ***serveurs hôtes distants*** redondants.

- Les spécialistes du soutien formés par Bayer s'authentifieront sur le ***serveur principal*** en utilisant un compte d'utilisateur attribué de manière unique et d'un mot de passe complexe, puis ils choisiront un produit Bayer et demanderont l'accès à distance. Le ***serveur principal*** acheminera la demande à l'un des deux ***serveurs hôtes distants*** pour lancer une séance à distance..

- L'***agent*** sondera périodiquement les ***serveurs hôtes distants*** pour détecter les demandes d'accès, déclenchant un second niveau d'authentification sur un appareil Bayer ou un logiciel déployé à l'aide d'un compte de soutien partagé de Bayer.

- En cas de réussite, l'***agent*** créera un tunnel chiffré inverse entre l'appareil ou le logiciel installé de Bayer et le spécialiste du soutien de Bayer à l'aide des ports sortants 443, 17001 et 17002. Cette connexion ne dépend pas d'adresses IP statiques ni des sous-réseaux.

Le saviez-vous?

- **Quelqu'un doit se trouver devant un appareil de Bayer pour permettre la connectivité au système d'exploitation de l'appareil ou à un système d'injection MEDRAD®.**

- **Les mises à jour des logiciels des appareils de Bayer peuvent être transférées du serveur principal de VirtualCARE ou d'une clé USB de Bayer par un ingénieur de service de Bayer sur place.**

- **Bayer suivra le processus de contrôle des changements du client pour toutes les activités de dépannage, de réparation, de mise à jour ou de maintenance.**

Sécurité

L'architecture de sécurité VirtualCARE 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 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 VirtualCARE au niveau de l'appareil de Bayer ou du logiciel installé, ainsi que sur le serveur principal de VirtualCARE.

Sécurité au niveau du réseau

- Le serveur hôte distant est visible par l'agent par l'entremise 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 par un fournisseur de soutien connu, ce qui élimine le risque de sécurité lié aux communications avec des utilisateurs inconnus.
- Un sondage des communications sur serveur (agent « ping ») permet de fournir des fichiers de données et rechercher une file d'attente des activités de maintenance prévues de VirtualCARE.
- VirtualCARE 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 à l'application VirtualCARE pour fournir 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.
- Seuls les spécialistes du soutien formés par Bayer de niveau 1, 2 ou 3 basés aux États-Unis peuvent lancer et contrôler une séance à distance. Dans un scénario de recours hiérarchique, un spécialiste du Canada peut également fournir du soutien de niveau 3. Si cela se produit, le client sera avisé et aura la possibilité de refuser une séance à distance amorcée par un spécialiste en poste à l'extérieur des États-Unis.
- À l'exception de ce qui est indiqué dans la documentation d'un produit particulier, aucun renseignement protégé sur l'état de santé des patients (IPS) n'est caché, traité ou stocké à l'extérieur d'un produit Bayer qui est hébergé et protégé par les mesures de protection physiques, techniques et administratives d'un 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 produits 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.

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 service de soutien de Bayer à VirtualCARE, 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 entièrement aux exigences de l'industrie des dispositifs médicaux, telles que définies par 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.**

Foire aux questions

Technologie

Q: Qu'est-ce que VirtualCARE?

R: La Radiologie de Bayer offre VirtualCARE pour assurer un accès à distance aux services d'installation, de surveillance, d'assistance, de maintenance et de mise à jour aux clients connectés dans le monde entier. VirtualCARE a été conçu pour améliorer les taux de résolution des problèmes dès la première visite grâce à un diagnostic avant la répartition et pour offrir aux clients un accès plus efficace à toutes les mises à jour logicielles qui peuvent être fournies à distance, dans le but de faciliter une reprise plus rapide en cas de panne.

Q:Comment Bayer active-t-elle VirtualCARE?

R: Bayer s'appuie sur ThingWorx, une technologie d'accès à distance de PTC, Inc., pour offrir les droits d'accès à VirtualCARE. En collaboration avec PTC, Bayer a examiné l'application ThingWorx afin de s'assurer de sa conformité aux politiques de Bayer qui régissent la sécurité et la protection des données.

Configuration

Q: Comment VirtualCARE est-il configuré?

R: L'agent VirtualCARE sera installé sur les appareils de Bayer. L'agent sondera périodiquement le serveur hôte distant pour détecter les demandes d'accès ou autres activités 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'appareil de Bayer. L'agent inversera un tunnel chiffré entre un spécialiste du soutien de Bayer et l'appareil de Bayer au moyen d'un protocole de chiffrement TLS de 128 bits.

Q: Quelles mesures le client doit-il prendre pour accéder à VirtualCARE?

R: Pour relier un système d'injection MEDRAD® à VirtualCARE, le client doit fournir un accès Internet sortant pour les URL medrad.axeda.com et bayer-prod-us-emsg. nuage. thingworx.com, et pour les ports 443, 17001 et 17002.

Q: Les équipements et logiciels des clients sont-ils constamment reliés à VirtualCARE?

R: Les appareils clients utilisent la méthode de sondage pour se connecter à l'application VirtualCARE; par conséquent, l'agent VirtualCARE sonde le serveur hôte distant toutes les 30 secondes.

Sécurité

Q: Comment l'architecture de sécurité de VirtualCARE est-elle conçue?

R: L'application VirtualCARE utilise des fonctions de sécurité à l'échelle de l'appareil, du réseau et de l'entreprise.

Q: Comment l'architecture de sécurité de VirtualCARE 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 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, VirtualCARE exige un certificat numérique pour valider le destinataire.

Q: Comment l'architecture de sécurité de VirtualCARE aborde-t-elle la sécurité de l'entreprise?

R: VirtualCARE permet uniquement aux spécialistes de soutien formés par Bayer basés aux États-Unis et au Canada d'établir des séances de soutien à distance. Les séances sont enregistrées sur le serveur hôte distant VirtualCARE et sur l'appareil ou le logiciel de Bayer. En outre, les séances sont consignées dans la base de données CRM de Bayer. VirtualCare ne fournit pas d'information d'identification pour accéder au réseau local (LAN) ou étendu (WAN) du client ou à des dispositifs ou logiciels autres que ceux de Bayer.

Q: L'application VirtualCARE conserve-t-elle des IPS

R: À l'exception de ce qui est indiqué dans la documentation d'un produit particulier, aucun renseignement protégé sur l'état de santé des patients (IPS) n'est caché, traité ou stocké à l'extérieur d'un produit Bayer qui est hébergé et protégé par les mesures de protection physiques, techniques et administratives d'un client.

Autres

Q: Mon établissement a besoin de documents pour confirmer que VirtualCARE 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.

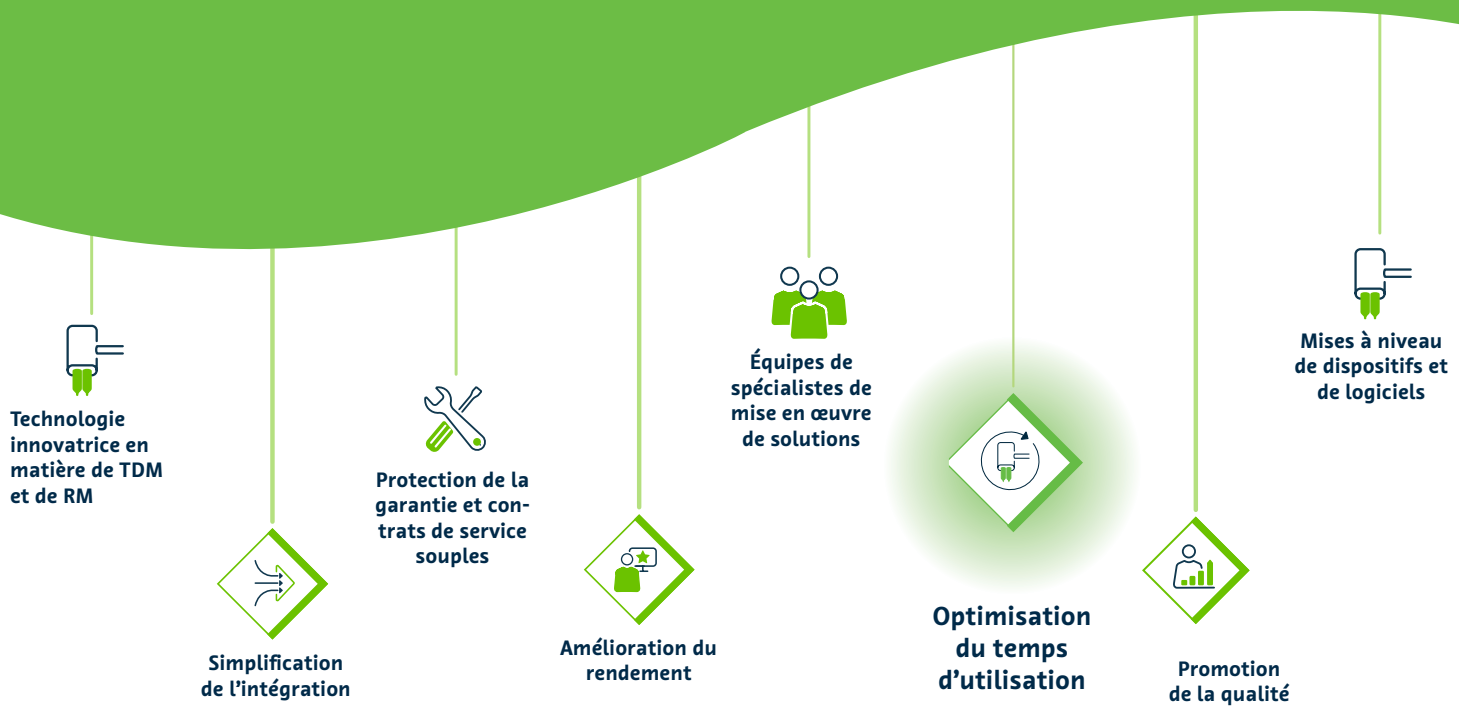
Q: Comment Bayer surveille-t-elle et évalue-t-elle les menaces de cybersécurité?

R: L'équipe de cybersécurité des dispositifs médicaux de radiologie maintient un programme rigoureux de surveillance et d'intervention pour les dispositifs et logiciels de Bayer. La page d'avis sur les technologies de l'information des services de radiologie fournit des mises à jour continues concernant la surveillance et les interventions en matière de cybersécurité à l'adresse suivante : https://www.radiologysolutions.bayer.com/information-technology-advisory.Services Information Technology Advisory page provides ongoing updates related to cybersecurity surveillance and response at: https://www.radiologysolutions.bayer.com/information-technology-advisory.

Ressources supplémentaires

Centres d'assistance technique de Bayer pour le soutien des dispositifs ou des logiciels

À chaque étape, Bayer offre des services de valeur, à vie



2920 Matheson Blvd East, Mississauga (Ontario) L4W 5R6
Téléphone : 1-800-268-1432
Télécopieur : 1-800-567-1710

PP-PF-RAD-CA-0724-1 Janvier 2023