

Lecture radiologique à distance : Comment gérer les risques de sécurité et garantir des performances optimales

Livre blanc

Par :

Jan Dobbenie

PDG de DOBCO Medical Systems

 +32 (52)77 01 16

 info@dobcomed.com

 Nachtegaalstraat 6, 9240 Zele Belgique

 www.pacsonweb.com

Table des matières

1. Introduction	3
2. Les risques de sécurité liés à la lecture à distance	4
2.1 Connexions VPN sur un PC ou un ordinateur portable personnel	4
2.2 Postes de travail détenus et gérés par les entreprises	6
2.3 VPN en combinaison avec des solutions de bureau virtuel	7
3. Défis en matière de logiciels et de bande passante : comparaison entre solution locale et solution cloud	8
4. PACS cloud sécurisé et entièrement accessible sur le Web	9
5. L'évolution de la plateforme Web cloud dans le domaine des soins de santé	11
6. PACSonWEB : le PACS cloud pour la lecture à distance et plus	12
7. Références	13

1. Introduction

Depuis de nombreuses années, les radiologues lisent des examens d'imagerie à domicile ou hors site. Au départ, il était possible d'accéder aux images depuis différents endroits de l'hôpital ou à partir d'un cabinet privé via un réseau local (LAN), connecté à un PACS (système d'archivage et de communication d'images) de l'hôpital. Aujourd'hui, les possibilités de lecture à distance se sont considérablement étoffées et les radiologues peuvent accéder aux images et à l'ensemble des fonctionnalités du PACS à domicile ou hors site via un WAN (réseau étendu).

La possibilité de lire des images en tout lieu à l'extérieur de l'hôpital s'est avérée particulièrement bénéfique en pleine pandémie de coronavirus, où la lecture à distance est apparue comme un moyen essentiel de favoriser la distanciation sociale et de protéger les radiologues, ainsi que les autres membres vulnérables de l'hôpital. En outre, la lecture à distance garantit des capacités d'interprétation continues dans les scénarios d'urgence, selon un article en libre accès publié avant l'impression par l'American Journal of Roentgenology (AJR).¹

Cependant, pour répondre aux demandes de lecture à distance, les organisations du secteur des soins de santé sont confrontées à plusieurs défis, qu'il s'agisse de fournir aux radiologues les bons outils à domicile ou d'offrir un environnement de travail sécurisé.

Dans ce livre blanc, nous examinerons les différentes options et les problèmes de sécurité, ainsi que les défis en matière de logiciels et de bande passante liés à la lecture à distance. Nous nous pencherons également sur l'évolution de la plateforme Web dans le cloud pour les soins de santé, et nous examinerons les avantages du PACS cloud.

« Aujourd'hui, les possibilités de lecture à distance se sont considérablement étoffées, et les radiologues peuvent accéder aux images et à l'ensemble des fonctionnalités du PACS à domicile ou hors site via un WAN. »

2. Les risques de sécurité liés à la lecture à distance

Les services informatiques sont aujourd'hui confrontés à un grand nombre de défis. La pénurie du personnel de sécurité technique, les exigences juridiques et de conformité réglementaire, ainsi que l'assaut constant de nouvelles menaces figurent parmi les défis majeurs en matière de sécurité, selon les experts en recherche et analyse de Gartner.² En outre, la COVID-19 a exercé une pression immense sur les organisations pour qu'elles étendent leurs initiatives de numérisation et adoptent le cloud computing.

Simultanément, les services informatiques du secteur des soins de santé sont allégés et couvrent une variété de responsabilités. Il n'est pas toujours possible d'évaluer rapidement pour doter le personnel médical d'ordinateurs portables ou d'appareils sécurisés et adaptés au travail, ce qui amène de nombreux radiologues à utiliser leurs dispositifs personnels (ordinateur portable, smartphone, tablette) pour se connecter à distance afin d'accéder aux données.

Quelle est la meilleure approche pour développer rapidement et efficacement la lecture à distance, tout en préservant la sécurité et en garantissant aux radiologues des niveaux de performances élevés du système ?

Nous examinerons d'abord l'utilisation d'une connexion à un réseau privé virtuel (VPN) dans diverses configurations.

2.1 Connexions VPN sur un PC ou un ordinateur portable personnel

« Bien que certains professionnels de la sécurité puissent considérer cette pratique [l'installation d'un VPN sur l'ordinateur personnel d'un employé] comme acceptable, cette politique est à haut risque avec un vecteur d'attaque indésirable lorsqu'elle permet l'accès à votre environnement. »

Morey Haber, The Dangers Of Using A VPN On Home Computers For Work And What To Do Instead, Forbes Technology Council ³

La COVID-19 a exercé une pression immense sur les organisations pour qu'elles étendent leurs initiatives de numérisation et adoptent le cloud computing. »

Une approche courante pour la lecture à distance consiste à fournir aux radiologues une connexion VPN qu'ils peuvent utiliser sur leur PC personnel à domicile ou sur leur ordinateur portable. Bien que cette option soit facile à mettre en place, elle présente plusieurs risques en matière de sécurité. Comme l'a souligné Morey Haber, voici quelques-unes des préoccupations essentielles :

A **La multiplicité des utilisateurs amplifie les risques**

Les ordinateurs personnels sont généralement partagés entre plusieurs membres de la famille. Si quelqu'un est victime de phishing (hameçonnage) ou d'un autre type d'attaque, il est possible qu'un virus soit téléchargé sur le réseau virtuel de l'organisation. Des techniques telles que le changement rapide d'utilisateur aggravent le problème en gardant d'autres profils en mémoire. En fin de compte, un utilisateur non lié à l'organisation pourrait facilement compromettre le réseau virtuel d'une organisation entière à cause d'une session VPN active connectée à l'organisation.

► **Incapacité à sécuriser l'hôte et absence d'autorité**

La plupart des solutions VPN d'entreprise intègrent généralement un certificat dans les profils des utilisateurs ou une connexion pour valider la connexion. Il s'agit d'une opération distincte de l'authentification que les utilisateurs doivent fournir par le biais des identifiants et d'une autre forme d'authentification à deux facteurs pour obtenir une connexion sécurisée. La sécurité du certificat et les informations d'identification pour l'authentification ne seront pas d'une grande utilité, car elles ne sont sûres que dans la mesure où le maintien de la sécurité est mis en œuvre par l'organisation. Celles-ci deviennent une cible privilégiée des cybercriminels, qui peuvent initier leurs propres connexions ou même détourner les sessions des employés à distance.

C'est un risque de sécurité majeur, car si vous ne parvenez pas à sécuriser l'hôte, vous ne parviendrez pas non plus à sécuriser le logiciel de connexion.



« Les ordinateurs personnels sont généralement partagés entre plusieurs membres de la famille. Si quelqu'un est victime de phishing (hameçonnage) ou d'un autre type d'attaque, il est possible qu'un virus soit téléchargé sur le réseau virtuel de l'organisation. »

De plus, si les solutions de contrôle d'accès au réseau peuvent effectivement valider les versions des signatures antivirus et les caractéristiques de base du matériel, elles ne sont pas en mesure de dresser l'inventaire d'un ordinateur domestique ni de s'assurer qu'il est entretenu et sécurisé comme un équipement de l'entreprise. Ces lacunes et cette absence d'autorité peuvent permettre la fuite de données provenant de logiciels malveillants de capture d'écran et d'enregistreurs de frappe.

► Une défense moindre contre les logiciels malveillants

La plupart des attaques de logiciels malveillants nécessitent des droits d'administration pour inspecter un système. Les utilisateurs de dispositifs personnels sont généralement des administrateurs locaux de leurs propres ordinateurs. Si les membres de l'équipe utilisent un système d'exploitation ancien, ils courent un risque plus important. Selon le rapport de sécurité 2019/2020 d' AV-TEST (institut de recherche indépendant sur la sécurité informatique en Allemagne), les ordinateurs qui fonctionnent sous Windows sont particulièrement vulnérables aux attaques : 114 millions de nouveaux programmes malveillants ont été développés en 2019, et 78,64 % de toutes les attaques ont été distribuées sur des systèmes Windows.⁴

► Absence de moyens de protection

Tout le monde ne se soucie pas d'avoir un logiciel antivirus à la maison. On estime que 25 % des PC ne sont pas protégés par un logiciel antivirus et qu'ils ont environ 5,5 fois plus de chances d'être infectés⁵. Bien que les utilisateurs de dispositifs personnels soient de plus en plus sensibilisés, bon nombre d'entre eux ne connaissent pas les outils de sécurité supplémentaires tels que la gestion des points d'extrémité, de la détection et de la réponse (EDR) ou la gestion des privilèges des points d'extrémité (EPM).

2.2 Postes de travail détenus et gérés par les entreprises

Certaines organisations de santé ont adopté l'approche consistant à fournir aux radiologues des postes de travail appartenant à l'entreprise et gérés par celle-ci. Cette solution permet d'assurer que les radiologues n'accèdent pas au

« Bon nombre d'utilisateurs ne connaissent pas les outils de sécurité supplémentaires tels que la gestion des points d'extrémité, de la détection et de la réponse (EDR) ou la gestion des privilèges des points d'extrémité (EPM). »

VPN de l'organisation par le biais d'ordinateurs de bureau traditionnels (à domicile).

Le poste de travail appartenant à l'entreprise fonctionne comme un poste de travail PACS ordinaire et pourrait même constituer un actif géré qui minimiserait les risques précédemment examinés.

Cependant, cette solution a un coût : ces postes de travail doivent être gérés et mis à jour par l'organisation, qui doit également fournir l'assistance nécessaire. Dans de nombreux cas, les organisations de santé ou les services informatiques ne sont pas organisés ou structurés pour assurer le support du matériel et des logiciels en dehors des murs de l'organisation, en particulier lorsqu'il s'agit du matériel et des logiciels spécialisés requis par les radiologues. Des ressources et des mesures supplémentaires sont nécessaires pour mettre à jour et gérer les systèmes afin de garantir la sécurité, les performances et le niveau de service nécessaire. Pour les radiologues, ces postes de travail sont le principal outil de lecture des examens et donc indispensables.

Par ailleurs, les performances peuvent toujours être problématiques et elles doivent être évaluées et testées, voire mises à l'épreuve, dans de multiples scénarios.

Généralement, les VPN fonctionnent sur une connexion Internet partagée avec l'organisation, ce qui signifie que les performances nécessaires ne peuvent être garanties en raison d'un manque de bande passante en amont de l'organisation de soins de santé.

2.3 VPN en combinaison avec des solutions de bureau virtuel

Il s'agit d'une solution très répandue dans les organisations de santé. Ces solutions (telles que Citrix, VirtualBox, Horizon et d'autres) créent un bureau virtuel sur l'ordinateur personnel du médecin avec un accès aux applications de l'organisation de soins de santé. Il s'agit d'un environnement isolé qui minimise les risques mentionnés précédemment. Ces solutions sont (en général) le bon choix du point de vue de la sécurité et, de plus, relativement faciles à mettre

« Les solutions (telles que Citrix, VirtualBox, Horizon et d'autres) créent un bureau virtuel sur l'ordinateur personnel du médecin avec un accès aux applications de l'organisation de soins de santé. »

en œuvre. Bien qu'elles soient très utiles pour la plupart des applications hospitalières nécessaires au domicile d'un médecin (par exemple pour accéder au DMI), elles ne sont pas adaptées à la lecture des examens dans le PACS. Le défilement de gros volumes de données, le réglage du contraste et de la brillance, la 3D ou la reconnaissance vocale ne sont tout simplement pas assez performants avec ce type de solution.

Il y a plusieurs raisons à cela : l'absence de prise en charge de plusieurs moniteurs, le taux de rafraîchissement de l'environnement, le manque de prise en charge de périphériques, etc. L'expérience générale indique que ces environnements ne sont pas assez performants pour exécuter des applications spécialisées telles que le PACS. En outre, l'affichage d'images DICOM sans perte en utilisant des techniques de bureau virtuel ou à distance comporte un risque potentiel, car l'image peut être compressée ou déformée par le logiciel de bureau virtuel.

3. Défis en matière de logiciels et de bande passante : comparaison entre solution locale et solution cloud

En plus des problèmes de sécurité, les équipes informatiques des soins de santé doivent gérer l'installation de plusieurs logiciels et les besoins en bande passante des radiologues pour effectuer des lectures à distance à partir de leurs appareils personnels. Un poste de travail PACS standard se compose de plusieurs moniteurs et nécessite l'installation de plusieurs applications logicielles telles que le logiciel PACS, le logiciel de reconnaissance vocale et le logiciel client du SIR (système d'information radiologique).

Ces applications sont généralement conçues pour des connexions LAN, car le PACS nécessite une connexion

« En revanche, les solutions PACS cloud accessibles sur le Web éliminent les risques de sécurité liés à l'utilisation d'un VPN, ne nécessitent l'installation d'aucun logiciel pour visualiser à distance des images DICOM sans perte de haute qualité et sont disponibles par tout navigateur sur tout appareil connecté à Internet. »

à large bande passante et à faible latence entre le client et le serveur en raison des gros volumes de données traités en vue d'un affichage fluide, en particulier pour les examens de tomodensitométrie et de résonance magnétique.

Par exemple, une simple tomodensitométrie peut atteindre plusieurs giga-octets. Le taux de rafraîchissement pour le rendu des images est également essentiel lorsque le radiologue effectue des manipulations, par exemple dans le cas du réglage du contraste et de la brillance des fenêtres. Si les radiologues peuvent opter pour une connexion Internet à plus large bande passante à domicile, la connexion de l'hôpital doit pouvoir également être en mesure de gérer la vitesse de chargement de plusieurs sessions à la fois pour les différentes applications.

Une approche que plusieurs fournisseurs de PACS ont mise en œuvre pour surmonter les problèmes de bande passante est la mise en cache des images sur le poste de travail. Dans de nombreux cas, le contenu du cache n'est pas crypté, ce qui entraîne des risques encore plus importants pour la sécurité et la confidentialité des données des patients, car ces mêmes données sont stockées sur les disques locaux. De plus, les connexions Internet sont sujettes à une latence élevée et à des coupures de connexion ; le logiciel du poste de travail PACS n'est pas conçu pour gérer ce type de situation.

Compte tenu de ces problèmes de sécurité, et de la nécessité de disposer de plusieurs applications logicielles d'imagerie médicale et d'une bande passante importante pour les radiologues, quelles sont les autres options permettant de développer rapidement et en toute sécurité la lecture à distance des radiographies ?

4. PACS cloud sécurisé et entièrement accessible sur le Web

Bien que l'utilisation d'un VPN, l'installation locale de logiciels et la mise à disposition d'un PC dédié aux

« Une simple tomodensitométrie peut atteindre plusieurs gigaoctets. »

radiologues puissent résoudre certains des problèmes de sécurité et de performance liés à la lecture à distance, cette approche comporte toujours des risques et nécessite une prise en charge importante de la part des services informatiques.

En revanche, les solutions PACS cloud accessibles sur le Web éliminent les risques de sécurité liés à l'utilisation d'un VPN, ne nécessitent l'installation d'aucun logiciel pour visualiser à distance des images DICOM sans perte de haute qualité et sont disponibles par tout navigateur sur tout appareil connecté à Internet.

Le client se limite à un navigateur qui communique via HTTPS avec l'environnement dans le nuage pour garantir la sécurité. Aucune donnée n'est laissée sur le PC ou le poste de travail local et il n'est pas nécessaire de gérer les clients. Ces solutions Web sécurisées mettent en œuvre des techniques d'authentification à plusieurs facteurs et une journalisation complète. Les mises à jour se limitent à l'environnement cloud et le logiciel fonctionne sur tout appareil ou système d'exploitation. À partir du cloud, les bandes passantes peuvent être adaptées et les connexions dupliquées pour assurer une disponibilité élevée.

La lecture à distance est entièrement prise en charge, et les radiologues peuvent :

- **Préparer des comptes rendus (préliminaires) hors des murs de l'hôpital, depuis leur domicile ou un autre bureau.**
- **Collaborer facilement avec d'autres groupes de lecture et des radiologues.**
- **Accéder à toutes les fonctionnalités du PACS sans avoir besoin d'un VPN ou d'une infrastructure informatique complexe.**

En outre, les images et les comptes rendus sont reliés en temps réel et le texte dicté s'affiche simultanément à l'écran. Une fois terminé, le compte rendu est intégré au système d'information radiologique (SIR) local ou au système de dossier médical électronique (DMI).

5. L'évolution de la plateforme Web cloud dans le domaine des soins de santé

Bien que le concept d'une plateforme Web cloud soit largement admis et mis en œuvre dans d'autres domaines (tels que la banque à domicile, les applications de bureau, la gestion de la relation client [CRM], etc.), l'adoption dans les domaines des logiciels informatiques médicaux, et des logiciels d'imagerie médicale en particulier, a été un peu plus lente (bien qu'elle gagne maintenant beaucoup de terrain). Plusieurs raisons expliquent ce phénomène :

➤ **Héritage** : les logiciels d'imagerie médicale sont traditionnellement des applications à client lourd qui nécessitent des ressources locales et ont des exigences spécifiques en matière de postes de travail. Les systèmes actuels sont développés à partir d'architectures et de techniques logicielles traditionnelles.

➤ **La barre technologique est haute pour mettre en œuvre chaque fonction dans un environnement Web** : de l'affichage de gros volumes de données CT/MR, d'outils d'imagerie complexes qui nécessitent une puissance de calcul (MIP/MPR), jusqu'à la reconnaissance vocale, chaque fonction est nécessaire pour soutenir le flux de travail du radiologue, mais elles sont difficiles à mettre en œuvre dans un environnement Web. La création de ces fonctions dans un contexte purement HTML exige beaucoup de R&D (en partant de zéro) et demande plus de choix (en matière de conception) qu'auparavant.

➤ **Nuage multilocataire** : Ce concept, bien qu'il ne soit pas encore très répandu dans le domaine des solutions de santé, car les fournisseurs se concentrent sur la seule entreprise, est assez courant dans d'autres secteurs (Salesforce, Google, etc.)

« Le concept d'une plateforme Web cloud est largement admis et mis en œuvre dans d'autres domaines (tels que les services bancaires à domicile, les applications de bureau, la gestion de la relation client [CRM], etc.) »

► **Performances** : Cette approche en ligne et dans le cloud nécessite de meilleures techniques, plus intelligentes, pour rendre les données plus rapidement disponibles sur des connexions à plus faible bande passante et à latence élevée.

Les avantages de cette technologie pour les soins de santé sont toutefois évidents. La technologie entièrement Web et cloud aidera les organisations (de soins de santé) à conserver et à simplifier leur infrastructure actuelle, à réduire les tâches de gestion et les coûts globaux, ainsi qu'à fournir une solution pour le travail à distance sans revoir à la baisse la politique de sécurité.

6. PACSonWEB : le PACS cloud pour la lecture à distance et plus

PACSonWEB est une solution cloud sécurisée, multilocataire et entièrement accessible sur le Web.

Les principales fonctions du PACS sont disponibles à tout moment, en tout lieu et sur tout appareil à partir de l'environnement cloud sécurisé. Le client est le navigateur et celui-ci communique en utilisant uniquement le protocole HTTPS. PACSonWEB prend en charge les applications avec plusieurs moniteurs et offre les fonctionnalités, la vitesse et la fluidité qu'un radiologue attend d'un poste de travail PACS, tout en maintenant le niveau de sécurité de l'organisation de santé. La lecture à distance avec reconnaissance vocale est intégrée et les tâches de gestion du service informatique sont considérablement réduites. Tous les utilisateurs de PACSonWEB, y compris les radiologues, les autres cliniciens, les médecins généralistes et les patients, bénéficient d'un soutien complet grâce à un service d'assistance centralisé, qui sert de point de contact unique pour toutes les questions relatives à PACSonWEB.

Cette assistance est disponible en anglais, en français, en allemand et en néerlandais, par téléphone, par courriel ou par un outil de connexion à distance tel que LogMeIn ou TeamViewer, avec des temps de réponse rapides garantis.

Si vous souhaitez en savoir plus sur PACSonWEB pour la lecture à distance ou obtenir davantage d'informations sur PACSonWEB, consultez :

www.pacsonweb.com

7. Références

1. Srinidhi Tridandapani, Greg Holl, et Cheri L. Canon, Rapid Deployment of Home PACS Workstations to Enable Social Distancing in the Coronavirus Disease (COVID-19) Era, American Journal of Roentgenology 2020 215:6, 1351-1353. Consulté à l'adresse : <https://www.ajronline.org/doi/full/10.2214/AJR.20.23495>

2. Christy Pettey, Gartner Top 9 Security and Risk Trends for 2020, 17 septembre 2020. Consulté à l'adresse : <https://www.gartner.com/smarterwithgartner/gartner-top-9-security-and-risk-trends-for-2020/>

3. Morey Haber, The Dangers Of Using A VPN On Home Computers For Work And What To Do Instead, Forbes, Forbes Technology Council, 17 juillet 2020, consulté à l'adresse : <https://www.forbes.com/sites/forbestechcouncil/2020/01/17/the-dangers-of-using-vpn-on-home-computers-for-work-and-what-to-do-instead/?sh=5041735d6349>

4. Rapport de sécurité AV-TEST 2019/2020, de l'institut de recherche indépendant AV-TEST pour la sécurité informatique en Allemagne, consulté à l'adresse : https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2019-2020.pdf

5. Sophie Anderson, Antivirus and Cybersecurity Statistics, Trends & Facts 2021, SafetyDetectives, 24 janvier 2020, consulté à l'adresse : [https://www.safetydetectives.com/blog/antivirus-statistics/#:~:text=The%20Threats%20Against%20Regular%20Users&text=However%2C%20an%20estimated%20one%2Dfourth,PUPs%20\(potentially%20unwanted%20programs\).](https://www.safetydetectives.com/blog/antivirus-statistics/#:~:text=The%20Threats%20Against%20Regular%20Users&text=However%2C%20an%20estimated%20one%2Dfourth,PUPs%20(potentially%20unwanted%20programs).)

DOBCO Medical Systems

Située en Belgique, DOBCO Medical Systems est spécialisée dans les solutions cloud d'imagerie médicale. La société a été fondée en 2011 par Jan Dobbenie et Kristof Coucke, deux vétérans du secteur des technologies de l'information dans le domaine de la santé, et a enregistré un chiffre d'affaires annuel de 4 millions d'euros en moins de huit ans.

Notre vision : Nous croyons au PACS dans le nuage informatique

Nous croyons fermement à la puissance de la technologie du Cloud et du Web pour améliorer les processus en radiologie et fournir des renseignements médicaux aux médecins et aux patients de manière plus efficace, plus rapide et plus sûre.

Notre objectif est de soutenir les radiologues afin qu'ils puissent améliorer leur service aux patients, aux médecins généralistes et aux cliniciens, ainsi qu'à la direction des hôpitaux.

Nous sommes des innovateurs. Nos solutions d'imagerie médicale sont conçues pour aider nos clients à atteindre les objectifs qu'ils se sont fixés en matière de soins aux patients, ainsi que leurs objectifs commerciaux, en leur offrant un meilleur service. Notre engagement : garantir une expérience et un service d'excellence à tous ceux qui accèdent aux images par la solution PACSonWEB, dans le cadre du continuum de soins aux patients.

Coordonnées

-  +32 (52)77 01 16
-  info@dobcomed.com
-  Nachtegaalstraat 6, 9240 Zele Belgique
-  www.pacsonweb.com