Guide des solutions réseau

SOINS DE SANTÉ

Alors que les coûts d'exploitation continuent d'augmenter, Allied Telesis est là pour s'assurer que vous fournissez à vos patients les solutions de soins de santé les plus sûres, les plus fiables et les plus efficaces.

Besoins et objectifs en matière de réseaux de soins de santé

49 % des prestataires de soins de santé sont en train de transformer leur modèle d'entreprise au cours des 12 prochains mois.

Source: Gartner Research, 2019

Le secteur des soins de santé subit des changements commerciaux et des bouleversements technologiques plus rapidement que tout autre grand secteur. Dans le monde entier, la demande de services de santé dépasse la capacité des prestataires de services à recevoir des patients et à fournir des soins personnels de haute qualité. Il y a une pénurie de professionnels de la santé et d'établissements de soins, en particulier dans les zones rurales ou isolées. Les coûts des soins de santé augmentent beaucoup plus vite que les revenus des particuliers et que la capacité des patients à payer, ce qui oblige les prestataires de soins à fournir des services à moindre coût.

L'aspect technologique de l'activité connaît des changements tout aussi importants. Une chambre d'hôpital moderne compte en moyenne 15 appareils en réseau qui surveillent l'état d'un patient et lui administrent des médicaments ou d'autres formes de soins. Les dossiers médicaux étant devenus numériques, les prestataires de soins ont besoin d'un accès mobile permanent au réseau pour accéder à ces dossiers et à d'autres informations pertinentes. De plus, de nombreux services sont proposés à distance via le réseau, notamment la télémédecine et les soins ambulatoires.

Les technologies disruptives, telles que l'IA, offriront des opportunités de créer de nouveaux modèles d'entreprise et de prestation de soins. Cependant, cela nécessitera une infrastructure plus agile, capable de répondre rapidement à l'évolution des nouveaux modèles de prestation de soins de santé qui peuvent répondre aux attentes accrues des consommateurs. C'est le défi auquel sont confrontés les prestataires de soins de santé.

Une autre perturbation est la décentralisation de l'infrastructure des soins de santé afin de réduire la distance entre le patient et le traitement. Si cette évolution est bénéfique pour le consommateur de soins de santé, elle accroît également la complexité des solutions informatiques.

Les éléments clés d'un réseau de soins de santé agile et à l'épreuve du temps sont les suivants :

Accès fiable à haut débit avec ou sans fil

Les prestataires de soins utilisant divers appareils mobiles doivent pouvoir accéder de manière fiable et sécurisée aux informations relatives aux patients, où qu'ils se trouvent, et disposer d'une bande passante suffisante pour l'imagerie médicale et la vidéo en temps réel. Les systèmes d'assistance aux patients, y compris la télémédecine et les moniteurs de santé à distance, ont besoin d'une connexion transparente sans interruption. L'accès à l'internet à haut débit pour les visiteurs doit également supporter un trafic à haute densité.

Sécurité globale

Les dossiers des patients contiennent des informations extrêmement sensibles et de grande valeur. Le réseau doit donc être protégé contre les accès non autorisés et les fuites ou vols de données.

Parallèlement à la cybersécurité, la sécurité physique doit être mise en œuvre pour protéger les biens et les patients.

Gestion aisée du réseau

Le réseau doit pouvoir gérer facilement les appareils câblés et sans fil sur site et hors site à partir d'un centre d'exploitation à distance.

Trouver un réseau qui réponde à tous vos besoins peut sembler une tâche impossible, mais avec une solution de réseau Allied Telesis adaptée à votre organisation, c'est à la fois réalisable et simple.

Priorités pour les réseaux de soins de santé

- Faciliter l'accès à l'information et aux ressources, tout en maintenant la sécurité des données confidentielles
- Fournir un accès sécurisé au réseau aux prestataires de soins et au personnel
- Fournir un accès Internet aux patients et aux membres de leur famille
- Protéger les données confidentielles des patients contre tout accès non autorisé
- Être prêt pour les applications commerciales émergentes
- Prise en charge et optimisation des connexions WAN multi-sites
- Être facile à configurer, à gérer et à dépanner, ce qui minimise les coûts d'administration et les temps d'arrêt
- Prise en charge de la gestion centralisée pour les sites distants dépourvus de ressources informatiques
- Assurer une récupération automatique en cas de défaillance d'un équipement ou d'une liaison, ainsi qu'en cas de boucles accidentelles

Solution Allied Telesis pour le secteur de la santé

Allied Telesis est un leader du secteur des solutions de réseau **robustes**.

Grâce à notre expérience éprouvée dans la fourniture de solutions réseau avancées hautement fiables et riches en fonctionnalités, de plus en plus de prestataires de soins de santé se tournent vers Allied Telesis pour atteindre leurs objectifs.

Allied Telesis met en œuvre des réseaux de soins de santé de pointe depuis de nombreuses années. Nous comprenons donc la nécessité de fournir des services de réseau avancés sans accroître la complexité opérationnelle. Notre portefeuille de produits et de services de grande valeur offre la sécurité, la mobilité et le réseau haute performance dont vous avez besoin, avec une gestion facile pour réduire les coûts d'exploitation, aujourd'hui et à l'avenir.

Voyons comment Allied Telesis relève les défis auxquels sont confrontés les soins de santé et fournit des solutions qui permettent d'obtenir de meilleurs résultats pour les patients et les entités qui les traitent.

Regarder vers l'avenir

Les produits Allied Telesis optimisent vos investissements technologiques en s'intégrant parfaitement aux systèmes et applications existants. Au fur et à mesure que de nouvelles applications commerciales sont développées, votre réseau peut facilement s'adapter car nos produits vous aident à construire une infrastructure plus efficace et plus progressive.

Alors que des technologies nouvelles et passionnantes sont mises en œuvre dans la fourniture de soins continus, les produits Allied Telesis restent à l'avant-garde en fournissant une infrastructure de réseau pour faciliter l'accès des patients aux meilleurs soins.

Accès imparable au réseau

Fournissez l'accès à tout moment en veillant à ce que votre réseau soit toujours opérationnel, même en cas de défaillance d'une liaison ou d'un équipement de réseau, sans intervention humaine.

Le réseau d'autodéfense

Notre sécurité intelligente protège votre réseau câblé et sans fil contre les menaces en mettant automatiquement en quarantaine les appareils suspects, créant ainsi un environnement sûr pour le stockage des données sensibles des patients.

Gestion fiable et facile du réseau étendu

Sélectionner le chemin optimal entre le bâtiment principal et les sites distants pour améliorer les performances et réduire les coûts.

Wi-Fi sans compromis

Garantir des connexions Wi-Fi fiables et performantes partout où elles sont nécessaires et assurer la prise en charge d'une densité élevée d'appareils pour l'équipement médical et l'accès du personnel soignant.

La gestion des réseaux en toute simplicité

Automatisez la gestion de votre réseau à l'aide d'un seul outil intelligent pour ajouter de l'intelligence et de la sécurité avec une gestion facile et pour réduire les risques et les coûts d'assistance tout en permettant une assistance sur site à distance.

Sécurité vidéo numérique

Portefeuille de produits dédiés au transport sécurisé et fiable de séquences vidéo sur le réseau IP.

ACCÈS AU RÉSEAU IMPARABLE

Le passage du papier aux dossiers médicaux électroniques concentre le flux d'informations au sein de l'infrastructure informatique. Parallèlement, le développement d'un système de soins de santé intégré exige une communication ininterrompue entre les différents hôpitaux et avec les cliniques et installations éloignées.

Au fur et à mesure de la mise en œuvre de cette transition, la haute disponibilité et l'accessibilité de l'infrastructure informatique deviennent vitales pour l'ensemble de l'écosystème des soins de santé.

La solution d'accès au réseau Allied Telesis unstoppable a été développée pour s'assurer que tout réseau est capable de survivre à des pannes multiples tout en maintenant la connectivité dans une large gamme d'architectures de réseau, fournissant ainsi une solution hautement disponible.

Dans un système complexe, la haute disponibilité doit prendre en compte de multiples facteurs, la haute disponibilité informatique n'étant qu'un des facteurs.

Alimentation de l'équipement de réseau

Dans l'hôpital, la continuité de l'alimentation électrique doit être garantie par l'utilisation d'une batterie de secours et d'un générateur automatisé. Les équipements de réseau peuvent se fier à cette source d'alimentation unique, mais ils doivent également être conçus pour résister à une défaillance du bloc d'alimentation interne.

Allied Telesis propose toute une série d'équipements dotés d'un système d'alimentation redondante, de sorte que si l'une des deux unités tombe en panne, l'équipement peut rester pleinement opérationnel, même en cas de panne de courant.

Alimentation simplifiée des dispositifs de réseau

Dans les hôpitaux, de nombreux appareils sont directement connectés à des commutateurs de réseau. L'utilisation d'équipements PoE pour alimenter ces appareils permet en outre de fournir une alimentation de secours au commutateur et d'alimenter les appareils connectés.

VCStack

VCStack et l'agrégation de liens offrent une solution où les ressources du réseau sont réparties entre les membres du châssis virtuel, ce qui garantit la résilience du dispositif et du chemin.

VCStack peut être déployé sur de longues distances, avec une connectivité par fibre optique. Un VCStack longue distance est parfait pour les environnements de réseaux distribués ou les solutions de miroirs de données.

Empilage virtuel

Plusieurs commutateurs Allied Telesis peuvent être connectés pour former un seul commutateur virtuel. Ensemble, la technologie d'empilage de châssis virtuels et l'agrégation de liens fournissent une solution résiliente capable de survivre à une défaillance de lien ou d'équipement.

Protection de l'anneau

Lorsque la distance entre les appareils est importante, une topologie en anneau pour le réseau est la solution optimale. Allied Telesis propose des protocoles de protection d'anneau pour protéger votre réseau contre les défaillances de liaison tout en fournissant une infrastructure résiliente.

Noyau redondant et reprise après sinistre

Dans le cas où un degré supplémentaire de résilience est nécessaire, Allied Telesis peut également fournir des commutateurs centraux avec une configuration redondante optimale pour une architecture de reprise après sinistre. Ceci est possible grâce à une pile virtuelle avec des équipements réseau situés dans différentes pièces ou même différents bâtiments.

EPSRing

Les solutions Ethernet Protection Switched Ring (EPSRing) d'Allied Telesis offrent des noyaux de réseaux distribués de haute performance, de haute fiabilité, flexibles et évolutifs.

Le temps de récupération en cas de défaillance des liaisons ou des nœuds est extrêmement rapide - 50 ms seulement -, ce qui rend cette solution idéale pour la fourniture d'un réseau de soins de santé avec des services de voix, de vidéo et de données.

CYBERSÉCURITÉ DES RÉSEAUX

Les cyber-attaques visant les établissements médicaux sont de plus en plus nombreuses et de plus en plus fréquentes. L'accès non autorisé aux données des patients, les ransomwares et d'autres types d'attaques affectent les opérations quotidiennes et entraînent un risque s

Le secteur des soins de santé doit impérativement assurer la sécurité des connexions internes aux ressources tout en permettant au personnel et aux visiteurs d'accéder à l'internet.

Les modèles de sécurité traditionnels qui se concentrent sur la prévention des attaques à l'intérieur du réseau ne sont pas suffisants car les attaques peuvent facilement venir de l'intérieur. Par exemple, un ordinateur portable, une tablette ou un appareil IoT infecté connecté au réseau peut constituer une menace sérieuse.

Parallèlement, les attaquants ont accru la sophistication de leurs méthodes et les menaces se présentent aujourd'hui sous des formes si diverses que le maintien d'un réseau sécurisé mais efficace est devenu un défi coûteux en temps et en argent.

Si l'approche traditionnelle basée sur le pare-feu est efficace pour détecter et bloquer les menaces et les virus provenant de l'internet, elle montre ses limites si l'attaque provient de l'intérieur du réseau. À ce stade, l'attaque se propage d'est en ouest sur le réseau (c'est-à-dire d'un appareil connecté à un autre), où elle ne peut être détectée par le pare-feu qu'une fois que la menace tente de franchir la frontière vers l'internet. Une fois la menace détectée, un administrateur peut être alerté et invité à entamer le processus de remédiation.

Malheureusement, ce processus dépend des ressources humaines, avec un temps de réaction qui peut aller de quelques minutes à quelques heures, voire quelques jours, en fonction de la disponibilité des ressources et de leurs compétences personnelles.

66%

des patients s'inquiètent du respect de la vie privée lorsque des informations sur la santé sont échangées par voie électronique.

Source: https://dashboard.healthit.gov

AMF-Sec

Pour permettre un réseau d'autodéfense qui aide les organisations à éviter les pertes de temps et les interruptions inutiles des services réseau, le contrôleur AMF-Sec est la clé de notre solution de sécurité AMF innovante et primée.

Caractéristiques principales :

- Compatible avec OpenFlow v1.3
- Convient aux réseaux câblés et sans fil
- Intégration avec les applications professionnelles pour gagner du temps et de l'argent
- Intégration avec les produits de sécurité pour détecter les menaces
- Le moteur Intelligent Isolation Adapter bloque automatiquement les menaces
- Évolutif - ajoutez plus d'applications d'entreprise pour une plus grande valeur ajoutée

Le réseau d'autodéfense

La solution Self-Defending Network offre une approche intégrée de la sécurité du réseau, automatisant les opérations informatiques manuelles et protégeant contre les menaces provenant des dispositifs d'accès câblés et sans fil.

Sans avoir besoin d'agents ou de logiciels pour les points finaux, le réseau d'autodéfense est capable de répondre automatiquement aux menaces dès qu'elles sont identifiées.

Les pare-feu et les dispositifs de sécurité identifient les menaces, puis le moteur intelligent mettant en œuvre la technologie Isolation Adapter intégrée dans notre contrôleur AMF-Sec réagit immédiatement pour isoler la partie du réseau affectée et mettre en quarantaine l'appareil suspect. Des mesures correctives peuvent être appliquées pour que l'appareil puisse réintégrer le réseau avec un minimum de perturbations. Les réponses sont configurables et la journalisation complète fournit une piste d'audit claire.

Le contrôleur AMF-Sec est la clé de notre solution de sécurité AMF innovante et primée. Il permet de créer un réseau autodéfensif qui aide les entreprises à éviter les pertes de temps et les interruptions inutiles des services réseau.

GESTION FIABLE ET FACILE DU RÉSEAU ÉTENDU

L'approche du secteur des soins de santé, centrée sur le patient, va dans le sens d'une décentralisation des services, les établissements de soins étant situés sur des sites locaux. Ces sites locaux doivent être connectés au réseau principal comme s'ils se trouvaient dans le même bâtiment hospitalier, avec un accès sécurisé et fiable.

En ce qui concerne l'infrastructure du réseau, la qualité de la connexion au site distant n'est pas une question triviale et doit être développée avec soin pour maintenir le même niveau de qualité que celui disponible dans l'hôpital principal. Les principaux problèmes liés à la fourniture d'une connexion à distance sont la disponibilité, le coût et la sécurité.

Il existe principalement deux options pour interconnecter des sites distants : une connexion dédiée louée avec un accord de niveau de service (SLA) spécifique, ou une liaison virtuelle privée sur un réseau public, câblé ou sans fil.

La première solution est plus coûteuse mais garantit la largeur de bande et la disponibilité de la liaison. La deuxième solution est moins coûteuse mais ne garantit pas la performance et la disponibilité.

Pour fournir un service de haute disponibilité, la meilleure option consiste à connecter les sites distants en utilisant plusieurs liaisons et à répartir le trafic entre elles en fonction de l'application, du coût de la liaison et d'autres paramètres. L'utilisation de liens multiples permet une sauvegarde en cas de défaillance et aboutit à une solution de haute disponibilité.

Pour sécuriser les données entre le site distant et l'hôpital principal, une liaison VPN sécurisée est toujours nécessaire. La gestion des liaisons multiples nécessite généralement une gestion complexe, impliquant fortement le service informatique pour tout changement nécessaire.

Gestion autonome et sécurisée du réseau étendu

Disposer de plusieurs connexions avec des performances et des coûts différents nécessite une attention permanente. Allied Telesis Software Defined WAN (SD-WAN) simplifie le contrôle des connexions des sites distants grâce à un outil de gestion autonome et centralisé.

SD-WAN Orchestrator fait partie de Vista Manager et gère de manière centralisée les connexions des succursales pour une mise à disposition fiable et sécurisée des applications. Il vous permet de définir des mesures de performance acceptables, d'optimiser et d'équilibrer automatiquement la fourniture d'applications et de surveiller facilement les performances du réseau étendu.

Le SD-WAN, avec les pare-feu Application-Aware d'Allied Telesis, fournit une solution intégrée de sécurité WAN et de gestion du trafic WAN dans un seul appareil.

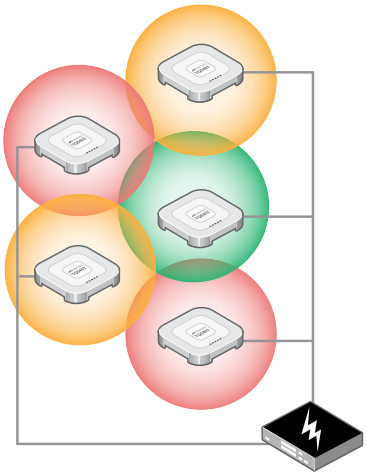
SD-WAN

Créez des réseaux étendus plus performants et plus sûrs, et améliorez votre productivité tout en réduisant la complexité et les coûts.

L'automatisation du WAN réduit le besoin de ressources qualifiées dans les succursales en centralisant l'optimisation et la surveillance des performances pour une gestion facile du WAN.

UNE CONNECTIVITÉ SANS FIL FIABLE

AWC



Allied Telesis Autonomous Wave Control (AWC) est une technologie réseau avancée qui utilise l'intelligence artificielle (IA) pour apporter des améliorations significatives à la connectivité et aux performances des réseaux sans fil tout en réduisant les coûts de déploiement et d'exploitation.

AWC surveille l'environnement Wi-Fi et optimise la couverture sans fil afin de fournir les meilleures performances possibles dans toutes les conditions.

Outre le fait que le personnel médical transporte des appareils mobiles d'une chambre à l'autre, un grand nombre d'appareils médicaux tels que les moniteurs de diagnostic d'images et les moniteurs portables nécessitent un réseau sans fil stable pour fournir des informations ou y accéder en temps réel.

Pour des raisons de sécurité, les appareils ayant accès aux données des patients exigent que l'utilisateur s'authentifie à nouveau dès que la connexion au réseau est interrompue. C'est pourquoi une solution sans fil ininterrompue et sans itinérance est considérée comme une valeur ajoutée pour le marché des soins de santé. Une connexion sans fil est également utilisée par les appareils médicaux comme liaison de secours en cas de défaillance de la connexion câblée, ce qui ajoute de la fiabilité à l'ensemble de la solution réseau.

Bien que le respect des normes techniques sans fil améliore les performances globales, il existe encore des limites qui nécessitent des compétences techniques approfondies pour mettre en œuvre un réseau sans fil stable. Dans un réseau sans fil, la déconnexion des clients et la lenteur des communications sont des problèmes typiques causés par un ou plusieurs problèmes techniques. Les interférences entre les canaux radio, les sources externes sans fil qui ne sont pas sous le contrôle du service informatique et la force du signal des points d'accès sont les principales raisons des problèmes sans fil.

Dans un environnement de soins de santé dynamique, il est essentiel de disposer d'un réseau continu avec des ressources informatiques de surveillance et qualifiées pour maintenir l'installation sous contrôle afin de fournir un service sans fil de qualité.

Wi-Fi sans compromis

La solution No Compromise Wi-Fi d'Allied Telesis garantit des connexions sans fil fiables et performantes partout où elles sont nécessaires sans augmenter les ressources qualifiées.

En analysant les lacunes de la couverture du signal et les interférences des points d'accès Wi-Fi, le contrôle autonome des ondes (AWC) offre automatiquement une expérience sans fil de haute qualité. Cela vous permet de réduire votre dépendance à l'égard d'ingénieurs réseau qualifiés et de bénéficier de coûts d'exploitation moindres.

AWC Channel Blanket (AWC-CB) permet de contrôler des points d'accès hybrides qui fournissent simultanément une connectivité Wi-Fi à un ou plusieurs canaux. Channel Blanket est la meilleure technologie radio pour fournir une connexion transparente aux appareils personnels et médicaux critiques lorsqu'ils se déplacent dans l'hôpital.

Les moniteurs de fréquence cardiaque, les capteurs de glycémie et les lits intelligents ne sont que quelques-uns des appareils mobiles qui ont besoin d'une connectivité sans fil fiable pour prodiguer les meilleurs soins aux patients. L'AWC-CB permet également de localiser les appareils afin de les retrouver facilement et de réduire la perte d'appareils coûteux.

GESTION SIMPLIFIÉE DU RÉSEAU

La complexité croissante des réseaux augmente considérablement les exigences en matière de gestion des réseaux et de ressources spécialisées. La mise en œuvre d'une solution d'automatisation simplifie et réduit le coût de la gestion du réseau.

Vista Manager EX is a modular single-pane-of-glass approach to network Vista Manager EX est une approche modulaire de la gestion de réseau. Il dispose d'un tableau de bord affichant les détails, l'état et les événements du réseau sur une carte topologique, et il met en évidence les problèmes critiques afin de minimiser le temps de réaction et d'aider à résoudre les problèmes en temps voulu sans avoir recours à des ingénieurs réseau hautement qualifiés.

Une série de modules pour contrôler le réseau câblé, les appareils sans fil, la liaison WAN et les outils d'automatisation facilitent la mise en réseau et rendent la solution modulaire.

Autonomous Management Framework Plus (AMF Plus)

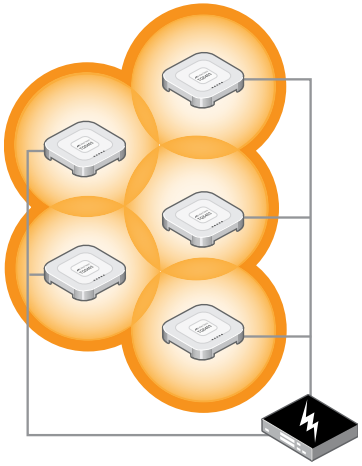
Réduire les coûts d'exploitation du réseau grâce à l'intelligence et à l'automatisation de la gestion centralisée.

Les services automatisés, y compris les mises à jour de micrologiciels, la sauvegarde, la récupération et l'approvisionnement sans contact ne sont que quelques-unes des caractéristiques de l'AMF Plus permettant de minimiser les ressources nécessaires à la gestion d'un réseau de soins de santé complexe.

Contrôle autonome des vagues (AWC) - module complémentaire

Analysez et optimisez les performances de réseaux sans fil complexes. Installez et oubliez votre réseau sans fil grâce à un outil autonome qui analyse les modèles de trafic et configure automatiquement les points d'accès pour répondre à la demande.

AWC-CB



Allied Telesis AWC Channel Blanket (AWC-CB) est la solution de canal unique pour le point d'accès sans fil Allied Telesis.

Tous les points d'accès membres de la même couverture fonctionnent sur le même canal. Le contrôleur intelligent AWC-CB gère les interférences et l'accès des clients.

Associé à l'approche multicanal traditionnelle, il constitue une solution complète d'accès sans fil pour tout type d'environnement.

AMF PLUS

Allied Telesis Autonomous Management Framework Plus (AMF Plus) est une plate-forme de gestion de réseau évolutive.

Il prend en charge les produits de commutation, de pare-feu et sans fil d'Allied Telesis, ainsi qu'une large gamme d'appareils tiers, notamment des caméras de vidéosurveillance et des téléphones IP, pour l'automatisation du réseau.

VISTA MANAGER™

Vista Manager EX offre une surveillance de pointe et crée automatiquement une carte topologique complète des commutateurs, des pare-feu et des points d'accès sans fil.

Avec la création et le mappage simplifiés des VLAN, l'analyse du trafic et les opérations SD-WAN, la gestion sans effort de tous les périphériques réseau est désormais une réalité.

VISTA MANAGER™ MINI

Une version de Vista Manager intégrée dans nos principaux commutateurs et pare-feu Allied Telesis offre une solution de gestion de réseau simple et rapide pour les petites et moyennes installations.

Sans nécessiter d'outils externes, Vista Manager Mini permet d'accéder facilement à la puissance de l'AMF Plus et de l'AWC pour la gestion des réseaux câblés et sans fil.

Réseau étendu défini par logiciel (SD-WAN)

Gérez de manière centralisée et optimisez automatiquement le trafic entre les succursales grâce au SD-WAN. Pour plus de détails, reportez-vous à la section "Gestion fiable et facile du réseau étendu".

Simple Network Management Protocol (SNMP) - module complémentaire

Auto-découverte et gestion d'une large gamme d'appareils dans un environnement multi-fournisseurs au sein de Vista Manager EX avec le module SNMP.

Différentes vues du réseau permettent d'obtenir la visibilité que vous souhaitez. Étendez la surveillance du réseau avec des notifications et des alertes automatisées pour une gestion proactive.

For more information please visit **alliedtelesis.com**

SÉCURITÉ PHYSIQUE

Les systèmes de contrôle d'accès aux bâtiments contribuent à protéger l'environnement physique de l'hôpital, mais pas entièrement. En effet, le grand nombre d'employés travaillant dans l'hôpital, de patients et de visiteurs entrant et sortant, rend difficile un contrôle total.

C'est pourquoi un système de vidéosurveillance avancé est nécessaire pour surveiller l'intérieur et l'extérieur de l'établissement médical et pour vérifier ce qui se passe dans des zones spécifiques.

Sécurité vidéo numérique

Dans toute mise en œuvre de vidéosurveillance, tous les dispositifs de stockage, les caméras de surveillance et les systèmes de gestion vidéo s'appuient sur l'infrastructure du réseau pour transporter la vidéo.

L'effet de la vidéosurveillance sur le réseau doit être pris en compte pour éviter un impact négatif sur la performance d'autres services.

Le trafic généré par les caméras IP, combiné au trafic existant sur les liaisons principales provenant des services, doit être calculé à l'avance pour garantir correctement une transmission fluide et fiable.

La partie principale de l'installation est alimentée par PoE avec une consommation électrique qui dépend de plusieurs facteurs comme le type de caméra et les accessoires (chauffage, moteurs, etc.). Lors de la phase de conception du réseau, les commutateurs d'accès connectés aux caméras IP doivent être sélectionnés de manière à pouvoir fournir suffisamment d'énergie pour alimenter toutes les caméras connectées.

Support ONVIF

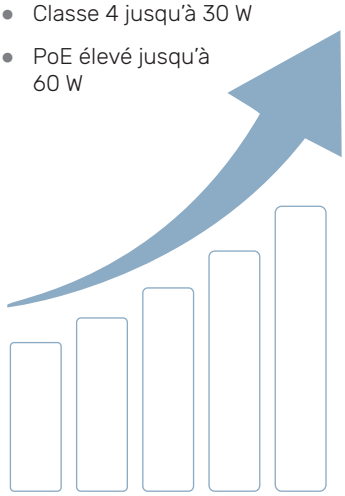
Allied Telesis a simplifié l'installation et la configuration des réseaux de vidéosurveillance en ajoutant la prise en charge des protocoles ONVIF à sa solution d'automatisation de réseau AMF Plus. Cela facilite le déploiement, la gestion et la maintenance des caméras de sécurité à distance.

Intégration des jalons

Le plug-in d'intégration Milestone est un complément au système XProtect VMS de Milestone System qui permet de contrôler directement les caméras IP connectées aux commutateurs Allied Telesis. Le plug-in simplifie la gestion des caméras à distance pour le personnel de sécurité en intégrant les tâches administratives courantes dans l'interface graphique de XProtect, ce qui permet d'économiser du temps et des appels coûteux.

Classe PoE

- Classe 0 jusqu'à 15 W
- Classe 1 jusqu'à 4 W
- Classe 2 jusqu'à 7 W
- Classe 3 jusqu'à 15 W
- Classe 4 jusqu'à 30 W
- PoE élevé jusqu'à 60 W



À PROPOS D'ALLIED TELESIS

Depuis plus de 30 ans, Allied Telesis fournit une connectivité fiable et intelligente aux entreprises et aux projets d'infrastructure complexes et critiques dans le monde entier.

Dans un monde qui évolue vers les villes intelligentes et l'Internet des objets, les réseaux doivent évoluer rapidement pour relever de nouveaux défis. Les technologies intelligentes d'Allied Telesis, telles qu'Allied Telesis Autonomous Management Framework™ Plus (AMF Plus) et Enterprise SDN, garantissent que l'évolution du réseau peut suivre le rythme et fournir des solutions efficaces et sécurisées pour les personnes, les organisations et les " choses ", aujourd'hui et à l'avenir.

Allied Telesis est reconnu pour avoir innové dans la manière dont les services et les applications sont fournis et gérés, ce qui se traduit par une augmentation de la valeur et une réduction des coûts d'exploitation.

Visitez-nous en ligne sur **alliedtelesis.com.**