

Guida alle soluzioni sanitarie

ASSISTENZA SANITARIA

Mentre i costi operativi continuano a crescere, Allied Telesis è qui per assicurarsi che stiate fornendo ai vostri pazienti le soluzioni sanitarie più sicure, affidabili ed efficienti.

Esigenze e obiettivi della rete sanitaria

49% dei fornitori di servizi sanitari sta per trasformare il proprio modello di business nei prossimi 12 mesi.

Fonte: Gartner Research, 2019

Il settore sanitario sta subendo cambiamenti aziendali e sconvolgimenti tecnologici più rapidamente di qualsiasi altro grande settore. In tutto il mondo, la domanda di servizi sanitari sta superando la capacità dei fornitori di servizi di visitare i pazienti e di fornire un'assistenza personale di alta qualità. C'è una carenza di professionisti e strutture sanitarie, soprattutto nelle zone rurali o remote. I costi dell'assistenza sanitaria aumentano molto più rapidamente dei redditi personali e della capacità di pagamento dei pazienti, mettendo i fornitori di servizi sanitari nella condizione di fornire servizi a costi inferiori.

Il lato tecnologico dell'attività sta subendo altrettanti cambiamenti. In una moderna stanza d'ospedale sono presenti in media 15 dispositivi collegati in rete che monitorano le condizioni del paziente e forniscono farmaci o altre forme di assistenza. Le cartelle cliniche sono diventate digitali e gli operatori hanno bisogno di un accesso mobile continuo alla rete per accedere a queste cartelle e ad altre informazioni rilevanti. Inoltre, molti servizi sono offerti in remoto attraverso la rete, tra cui la telemedicina e l'assistenza ambulatoriale.

Le tecnologie dirompenti, come l'intelligenza artificiale, offriranno l'opportunità di creare nuovi modelli di business e di erogazione delle cure. Tuttavia, ciò richiederà un'infrastruttura più agile, in grado di rispondere rapidamente all'evoluzione di nuovi modelli di erogazione dell'assistenza sanitaria in grado di soddisfare le crescenti aspettative dei consumatori. Questa è la sfida che devono affrontare i fornitori di servizi sanitari.

Un'altra perturbazione è la decentralizzazione dell'infrastruttura sanitaria per ridurre la distanza tra il paziente e le cure. Se da un lato ciò va a vantaggio del consumatore di assistenza sanitaria, dall'altro aggiunge complessità alle soluzioni IT.





Gli elementi chiave di una rete sanitaria agile e a prova di futuro sono:



Accesso affidabile ad alta velocità via cavo e wireless

Gli operatori sanitari che utilizzano una varietà di dispositivi mobili devono poter accedere in modo affidabile e sicuro alle informazioni sui pazienti da qualsiasi luogo, con una larghezza di banda sufficiente per immagini e video medici in tempo reale. I sistemi di assistenza ai pazienti, tra cui la telemedicina e i monitor sanitari remoti, necessitano di una connessione continua senza interruzioni. L'accesso a Internet ad alta velocità per gli ospiti deve anche supportare un traffico ad alta densità.



Sicurezza generale

Le cartelle cliniche dei pazienti contengono informazioni estremamente sensibili e di alto valore. Pertanto, la rete deve essere protetta da accessi non autorizzati e da fughe di dati o furti.

Parallelamente alla cybersecurity, è necessario implementare la sicurezza fisica per proteggere i beni e i pazienti.



Facile gestione della rete

La rete deve gestire facilmente i dispositivi cablati e wireless sia in sede che fuori sede da un centro operativo remoto.

Trovare una rete che soddisfi tutte le vostre esigenze può sembrare un compito impossibile, ma con una soluzione di rete Allied Telesis su misura per la vostra organizzazione, è possibile e semplice.

Priorità per le reti sanitarie:

- Facilitare l'accesso alle informazioni e alle risorse, mantenendo la sicurezza dei dati riservati
- Fornire un accesso sicuro alla rete ai fornitori di cure e al personale
- Fornire l'accesso a Internet ai pazienti e ai familiari
- Proteggere i dati riservati dei pazienti da accessi non autorizzati
- Essere pronti per le applicazioni aziendali emergenti
- Supporto e ottimizzazione delle connessioni WAN multi-sito
- Essere facili da configurare, gestire e risolvere i problemi, riducendo al minimo i costi di amministrazione e i tempi di inattività
- Supporto della gestione centralizzata per siti remoti senza risorse IT
- Fornisce un ripristino automatico in caso di guasto dell'apparecchiatura o del collegamento, nonché in caso di loop accidentali

Soluzione Allied Telesis per il settore sanitario

Allied Telesis è un leader del settore nelle soluzioni di rete robuste.

Grazie alla nostra comprovata esperienza nella fornitura di soluzioni di rete avanzate altamente affidabili e ricche di funzionalità, un numero sempre maggiore di strutture sanitarie si rivolge ad Allied Telesis per raggiungere i propri obiettivi.

Allied Telesis ha implementato reti sanitarie all'avanguardia per molti anni, quindi comprende la necessità di fornire servizi di rete avanzati senza aumentare la complessità operativa. Il nostro portafoglio di prodotti e servizi di alto valore fornisce la sicurezza, la mobilità e le alte prestazioni di cui avete bisogno, con una gestione semplice per ridurre i costi operativi, sia ora che in futuro.

Vediamo come Allied Telesis affronta le sfide del settore sanitario e fornisce soluzioni che consentono di ottenere risultati migliori per i pazienti e gli enti che li curano.

Guardare al futuro

I prodotti Allied Telesis ottimizzano i vostri investimenti tecnologici grazie alla completa integrazione con i sistemi e le applicazioni esistenti. Man mano che vengono sviluppate nuove applicazioni aziendali, la vostra rete può facilmente adattarsi e i nostri prodotti vi aiutano a costruire un'infrastruttura più efficiente e all'avanguardia.

Con l'implementazione di nuove ed entusiasmanti tecnologie per l'erogazione di cure continue, i prodotti Allied Telesis rimangono all'avanguardia nel fornire un'infrastruttura di rete che faciliti l'accesso dei pazienti alle cure migliori.



Accesso alla rete inarrestabile

Fornite l'accesso in qualsiasi momento, assicurando che la rete sia sempre attiva e funzionante, anche in caso di guasti ai collegamenti o alle apparecchiature di rete, senza la necessità di un intervento umano.



La rete di autodifesa

La nostra sicurezza smart edge protegge la rete cablata e wireless dalle minacce mettendo automaticamente in quarantena i dispositivi sospetti, creando così un ambiente sicuro per l'archiviazione dei dati sensibili dei pazienti.



Gestione WAN affidabile e semplice

Selezionare il percorso ottimale tra l'edificio principale e i siti remoti per ottenere prestazioni migliori e costi inferiori.



Wi-Fi senza compromessi

Garantisce connessioni Wi-Fi affidabili e ad alte prestazioni ovunque siano necessarie e fornisce un supporto ad alta densità di dispositivi per le apparecchiature mediche e l'accesso degli operatori.



Gestione della rete semplificata

Automatizzate la gestione della rete utilizzando un unico strumento intelligente per aggiungere intelligenza e sicurezza con una gestione semplice e per ridurre i rischi e i costi di supporto, consentendo l'assistenza in remoto.



Sicurezza video digitale

Portafoglio di prodotti dedicati per il trasporto sicuro e affidabile di filmati attraverso la rete IP.



ACCESSO ALLA RETE INARRESTABILE



Il passaggio dalla carta alla cartella clinica elettronica concentra il flusso di informazioni all'interno dell'infrastruttura informatica. Allo stesso tempo, lo sviluppo di un sistema sanitario integrato richiede una comunicazione ininterrotta tra i diversi ospedali e con le cliniche e le strutture remote.

Con la piena attuazione di questa transizione, l'alta disponibilità e l'accessibilità dell'infrastruttura informatica diventano fondamentali per l'intero ecosistema sanitario.

La soluzione di accesso alla rete inarrestabile di Allied Telesis è stata sviluppata per garantire che qualsiasi rete sia in grado di sopravvivere a più guasti mantenendo la connettività in un'ampia gamma di architetture di rete, fornendo così una soluzione ad alta disponibilità.

All'interno di un sistema complesso, l'alta disponibilità deve considerare molteplici fattori, dove l'alta disponibilità informatica è solo uno dei fattori.

Alimentazione delle apparecchiature di rete

In ospedale, la continuità dell'alimentazione deve essere garantita da una batteria di backup e da un generatore automatico. Le apparecchiature di rete possono affidarsi a questa unica fonte di alimentazione, ma devono anche essere progettate per resistere in caso di guasto dell'alimentatore interno.

Allied Telesis propone un'intera serie di apparecchiature con un sistema di alimentazione ridondante, in modo che se una delle due unità si guasta, l'apparecchiatura può rimanere pienamente operativa, anche in caso di blackout.



Alimentazione semplificata dei dispositivi di rete

Molti dispositivi negli ospedali sono collegati direttamente agli switch di rete. L'uso di apparecchiature abilitate PoE per l'alimentazione di questi dispositivi consente inoltre di fornire alimentazione di backup allo switch e di restituire l'alimentazione ai dispositivi collegati.

VCSTACK

VCStack e l'aggregazione di link forniscono una soluzione in cui le risorse di rete sono distribuite tra i membri dello chassis virtuale, garantendo la resilienza del dispositivo e del percorso.

Il VCStack può essere distribuito su lunghe distanze, con connettività in fibra. Un VCStack a lunga distanza è perfetto per gli ambienti di rete distribuiti o per le soluzioni di mirroring dei dati.

Impilamento virtuale

Più switch Allied Telesis possono essere collegati per formare un unico switch virtuale. Insieme, la tecnologia Virtual Chassis Stacking con Link Aggregation fornisce una soluzione resiliente in grado di sopravvivere a un guasto del collegamento o dell'apparecchiatura.

Protezione dell'anello

Quando la distanza tra i dispositivi è elevata, una topologia ad anello per la rete è la soluzione ottimale. Allied Telesis offre protocolli di protezione ad anello per proteggere la rete da guasti ai collegamenti e fornire un'infrastruttura resiliente.

Nucleo ridondante e disaster recovery

Nel caso in cui sia necessario un ulteriore grado di resilienza, Allied Telesis può anche fornire switch core con una configurazione ridondante ottimale per un'architettura di disaster recovery. Ciò è possibile grazie a uno stack virtuale con dispositivi di rete situati in stanze o addirittura edifici diversi.

EPSRING

Le soluzioni Allied Telesis Ethernet Protection Switched Ring (EPSRing) forniscono prestazioni elevate, alta affidabilità e nuclei di rete distribuiti flessibili e scalabili.

Il tempo di ripristino in caso di interruzione dei collegamenti o dei nodi è estremamente rapido, pari a 50 ms, e rende questa soluzione ideale per la fornitura di una rete sanitaria con servizi voce, video e dati.





CYBERSICUREZZA DI RETE

Gli attacchi informatici alle istituzioni mediche sono in aumento e sempre più frequenti. L'accesso non autorizzato ai dati dei pazienti, il ransomware e altri tipi di attacchi compromettono le operazioni quotidiane e mettono a serio rischio la privacy dei pazienti.

Mantenere sicure le connessioni interne alle risorse, consentendo al contempo l'accesso a Internet al personale e agli ospiti, è obbligatorio per il settore sanitario.

I modelli di sicurezza tradizionali che si concentrano sulla prevenzione degli attacchi dall'interno della rete non sono sufficienti, poiché gli attacchi possono facilmente provenire dall'interno. Ad esempio, un laptop, un tablet o un dispositivo IoT infetto collegato alla rete può rappresentare una seria minaccia.

Parallelamente, gli aggressori hanno aumentato la sofisticazione dei loro metodi e ora le minacce si presentano in così tante forme che mantenere una rete sicura ma efficace è diventata una sfida lunga e costosa.

Mentre l'approccio tradizionale basato sul firewall è efficace per rilevare e bloccare le minacce e i virus provenienti da Internet, mostra i suoi limiti se l'attacco proviene dall'interno della rete. In questa fase, l'attacco si diffonderà in direzione est/ovest sulla rete (cioè da un dispositivo connesso a un altro), dove potrà essere rilevato dal firewall solo quando la minaccia cercherà di attraversare il confine con Internet. Una volta rilevata la minaccia, è possibile avvisare un amministratore e chiedergli di iniziare il processo di bonifica.

Purtroppo questo processo dipende dalle risorse umane, con tempi di reazione che possono andare dai minuti alle ore o addirittura ai giorni, a seconda della disponibilità delle risorse e delle competenze personali.

La rete di autodifesa

La soluzione Self-Defending Network fornisce un approccio integrato alla sicurezza della rete, automatizzando le operazioni IT manuali e proteggendo dalle minacce provenienti da dispositivi di accesso sia cablati che wireless.

Senza bisogno di agenti o software per gli endpoint, la Self-Defending Network è in grado di rispondere automaticamente alle minacce una volta identificate.

66%

dei pazienti ha problemi di privacy quando le informazioni sanitarie vengono scambiate elettronicamente.

Fonte: <https://dashboard.healthit.gov>

AMF-SEC

Per consentire una rete autodifesa che aiuti le aziende a evitare perdite di tempo e inutili interruzioni dei servizi di rete, il controller AMF-Sec è la chiave della nostra innovativa e pluripremiata soluzione AMF Security.

Caratteristiche principali:

- Compatibile con OpenFlow v1.3
- Adatto per reti cablate e wireless
- Si integra con le applicazioni aziendali per risparmiare tempo e denaro
- Si integra con i prodotti di sicurezza per rilevare le minacce
- Il motore dell'adattatore di isolamento intelligente blocca automaticamente le minacce
- Scalabile: aggiungere altre app aziendali per un valore maggiore

I firewall e le appliance di sicurezza identificano le minacce, quindi il motore intelligente che implementa la tecnologia Isolation Adapter integrata nel nostro controller AMF-Sec risponde immediatamente per isolare la parte di rete interessata e mettere in quarantena il dispositivo sospetto. È possibile applicare una correzione in modo che il dispositivo possa rientrare nella rete con un'interruzione minima. Le risposte sono configurabili e la registrazione completa fornisce una chiara traccia di audit.

Per consentire una rete autodifesa che aiuti le aziende a evitare perdite di tempo e inutili interruzioni dei servizi di rete, il controller AMF-Sec è la chiave della nostra innovativa e pluripremiata soluzione AMF Security.





GESTIONE WAN AFFIDABILE E SEMPLICE



L'approccio del settore sanitario incentrato sul paziente segue la direzione del decentramento dei servizi, in cui le strutture di cura sono situate in siti locali. Questi siti locali devono essere collegati alla rete principale come se si trovassero nello stesso edificio ospedaliero, con un accesso sicuro e affidabile.

Per quanto riguarda l'infrastruttura di rete, la qualità della connessione al sito remoto non è una questione banale e deve essere sviluppata con attenzione per mantenere lo stesso livello di qualità disponibile nell'ospedale principale. I problemi principali nel fornire una connessione remota sono la disponibilità, il costo e la sicurezza.

Esistono principalmente due opzioni per interconnettere i siti remoti: una connessione dedicata in affitto con uno specifico Service Level Agreement (SLA), oppure un collegamento virtuale privato su una rete pubblica, cablata o wireless.

La prima soluzione è più costosa ma garantisce la larghezza di banda e la disponibilità del collegamento. La seconda soluzione è meno costosa ma non garantisce prestazioni e disponibilità.

Per fornire un servizio ad alta disponibilità, l'opzione migliore è quella di collegare i siti remoti utilizzando più collegamenti e suddividere il traffico tra di essi in base all'applicazione, al costo del collegamento e ad altri parametri. L'uso di più collegamenti consente di avere un backup in caso di guasto e di ottenere una soluzione ad alta disponibilità.

Per proteggere i dati tra il sito remoto e l'ospedale principale, è sempre necessario un collegamento VPN sicuro. La gestione dei collegamenti multipli richiede solitamente una gestione complessa, che coinvolge pesantemente il reparto IT per qualsiasi modifica necessaria.

Gestione autonoma e sicura della WAN

Disporre di più connessioni con prestazioni e costi diversi richiede un'attenzione continua. Allied Telesis Software Defined WAN (SD-WAN) semplifica il controllo delle connessioni dei siti remoti con uno strumento di gestione autonomo e centralizzato.

SD-WAN Orchestrator fa parte di Vista Manager e gestisce centralmente le connessioni delle filiali per una distribuzione affidabile e sicura delle applicazioni. È possibile impostare metriche di performance accettabili, ottimizzare e bilanciare automaticamente la distribuzione delle applicazioni e monitorare facilmente le prestazioni della WAN.

SD-WAN, con i firewall Allied Telesis Application-Aware, fornisce una soluzione integrata di sicurezza e gestione del traffico WAN in un unico dispositivo.

SD-WAN

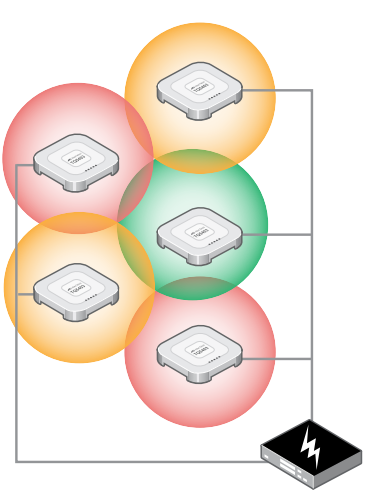
Realizzate WAN più performanti e sicure e migliorate la produttività riducendo la complessità e i costi.

L'automazione della WAN riduce la necessità di risorse qualificate presso la filiale, centralizzando l'ottimizzazione delle prestazioni e il monitoraggio per una facile gestione della WAN.

CONNETTIVITÀ WIRELESS AFFIDABILE



AWC



L'Autonomous Wave Control (AWC) di Allied Telesis è una tecnologia di rete avanzata che utilizza l'intelligenza artificiale (AI) per offrire miglioramenti significativi nella connettività e nelle prestazioni della rete wireless, riducendo al contempo i costi di implementazione e di gestione.

AWC monitora l'ambiente Wi-Fi e ottimizza la copertura wireless per fornire le migliori prestazioni possibili in qualsiasi condizione.

Oltre al personale medico che trasporta dispositivi mobili da una stanza all'altra, un gran numero di dispositivi medici, come i monitor per la diagnostica delle immagini e i monitor indossabili, richiedono una rete wireless stabile per fornire o accedere alle informazioni in tempo reale.

Per motivi di sicurezza, i dispositivi che hanno accesso ai dati dei pazienti richiedono all'utente una nuova autenticazione una volta che la connessione di rete cade. Per questo motivo, una soluzione wireless senza roaming ininterrotto è considerata un valore aggiunto per il mercato sanitario. Una connessione wireless viene inoltre utilizzata dai dispositivi medici come collegamento di backup in caso di guasto della connessione cablata, aggiungendo affidabilità all'intera soluzione di rete.

Sebbene gli standard tecnici wireless migliorino le prestazioni complessive, esistono ancora limitazioni che richiedono competenze tecniche approfondite per implementare una rete wireless stabile. In una rete wireless, la disconnessione dei client e la lentezza delle comunicazioni sono problemi tipici del wireless, solitamente causati da uno o più problemi tecnici. Le interferenze tra i canali radio, le fonti wireless esterne non controllate dall'IT e la potenza del segnale dei punti di accesso sono le ragioni principali dei problemi wireless.

In un ambiente sanitario dinamico, è fondamentale la necessità di una rete continua con monitoraggio e risorse informatiche qualificate per mantenere l'installazione sotto controllo e fornire un servizio wireless di valore.

Wi-Fi senza compromessi

La soluzione Wi-Fi No Compromise di Allied Telesis garantisce connessioni wireless affidabili e ad alte prestazioni ovunque siano necessarie senza aumentare le risorse qualificate.

Analizzando le lacune nella copertura del segnale e le interferenze dei punti di accesso Wi-Fi, l'Autonomous Wave Control (AWC) offre automaticamente un'esperienza wireless di alta qualità. Ciò consente di ridurre la dipendenza da tecnici di rete qualificati e di ridurre i costi operativi.

AWC Channel Blanket (AWC-CB) consente il controllo di punti di accesso ibridi che forniscono simultaneamente connettività Wi-Fi singola e multicanale. Channel Blanket è la migliore tecnologia radio per fornire una connessione continua ai dispositivi medici e personali critici mentre si spostano all'interno dell'ospedale.

Cardiofrequenzimetri, sensori di glicemia e letti intelligenti sono solo alcuni dei dispositivi mobili che necessitano di una connettività wireless affidabile per la migliore assistenza ai pazienti. AWC-CB consente inoltre di localizzare i dispositivi per trovare facilmente le apparecchiature e ridurre la perdita di dispositivi costosi.

GESTIONE SEMPLIFICATA DELLA RETE



La crescente complessità della rete aumenta in modo significativo le richieste di gestione della rete e di risorse specializzate. L'implementazione di una soluzione di automazione semplifica e riduce i costi di gestione della rete.

Vista Manager EX è un approccio modulare a un unico pannello di vetro per la gestione della rete. Dispone di un cruscotto che mostra i dettagli della rete, lo stato e gli eventi su una mappa della topologia e mette in evidenza i problemi critici per ridurre al minimo i tempi di reazione e aiutare a risolvere i problemi in modo tempestivo senza dover ricorrere a tecnici di rete altamente qualificati.

Una serie di moduli per il controllo della rete cablata, dei dispositivi wireless, del collegamento WAN e degli strumenti di automazione rendono il collegamento in rete semplice e la soluzione modulare.

Autonomous Management Framework Plus (AMF Plus)

Riducete i costi operativi della rete grazie all'intelligenza e all'automazione della gestione centralizzata.

I servizi automatizzati, tra cui gli aggiornamenti del firmware, il backup, il ripristino e il provisioning zero-touch, sono solo alcune delle caratteristiche di AMF Plus che riducono al minimo le risorse necessarie per gestire una rete sanitaria complessa.

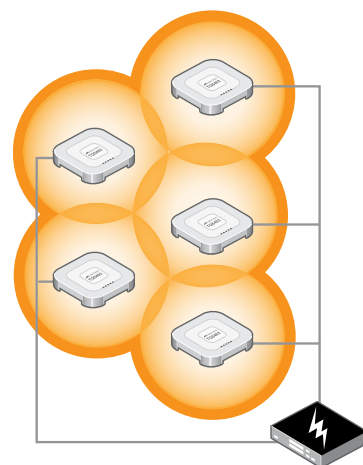
Controllo autonomo dell'onda (AWC) - modulo aggiuntivo

Analizzate e ottimizzate le prestazioni di reti wireless complesse. Installate e dimenticate la vostra rete wireless con uno strumento autonomo che analizza i modelli di traffico e configura automaticamente i punti di accesso per soddisfare la domanda.

WAN definita dal software (SD-WAN)

Gestite centralmente e ottimizzate automaticamente il traffico tra le filiali con SD-WAN. Per maggiori dettagli, consultare la sezione "Gestione affidabile e semplice della WAN".

AWC-CB



Allied Telesis AWC Channel Blanket (AWC-CB) è la soluzione a canale singolo per il punto di accesso wireless Allied Telesis.

Tutti gli access point che fanno parte della stessa coperta operano sullo stesso canale. Il controller intelligente AWC-CB gestisce le interferenze e l'accesso dei client.

Insieme al tradizionale approccio multi-canale, fornisce una soluzione di accesso wireless completa per qualsiasi ambiente.

AMF PLUS

Allied Telesis Autonomous Management Framework Plus (AMF Plus) è una piattaforma di gestione di rete scalabile.

Supporta i prodotti di commutazione, firewall e wireless di Allied Telesis, nonché un'ampia gamma di dispositivi di terze parti, tra cui telecamere di videosorveglianza e telefoni IP, per l'automazione della rete.

Simple Network Management Protocol (SNMP) - modulo aggiuntivo

Scoprite e gestite automaticamente un'ampia gamma di dispositivi in un ambiente multi-vendor all'interno di Vista Manager EX con il componente aggiuntivo SNMP.

Diverse visualizzazioni della rete consentono la visibilità nel modo preferito. Estendete il monitoraggio della rete con notifiche e avvisi automatici per una gestione proattiva.

VISTA MANAGER™

Vista Manager EX offre un monitoraggio all'avanguardia e crea automaticamente una mappa topologica completa di switch, firewall e AP wireless.

Con la creazione e la mappatura semplificata delle VLAN, l'analisi del traffico e le operazioni SD-WAN, la gestione senza sforzo di tutti i dispositivi di rete è ora una realtà.

VISTA MANAGER™ MINI

Una versione di Vista Manager integrata nei nostri switch e firewall Allied Telesis di base offre una soluzione di gestione della rete facile e veloce per le installazioni di piccole e medie dimensioni.

Una versione di Vista Manager integrata nei nostri switch e firewall Allied Telesis di base offre una soluzione di gestione della rete facile e veloce per le installazioni di piccole e medie dimensioni.





SICUREZZA FISICA



I sistemi di controllo degli accessi agli edifici aiutano a proteggere l'ambiente fisico dell'ospedale, ma non completamente. Questo è dovuto alla grande quantità di personale che lavora nell'ospedale e di pazienti e visitatori che entrano ed escono, rendendo difficile un controllo completo.

Per questo motivo, è necessario un sistema di videosorveglianza avanzato per monitorare sia l'interno che l'esterno della struttura medica e per verificare ciò che accade in aree specifiche.

Sicurezza video digitale

In qualsiasi implementazione di videosorveglianza, tutti i dispositivi di archiviazione, le telecamere di sorveglianza e i sistemi di gestione video si affidano all'infrastruttura di rete per il trasporto dei video.

L'effetto della videosorveglianza sulla rete deve essere considerato per evitare un impatto negativo sulle prestazioni di altri servizi.

Il traffico generato dalle telecamere IP, in combinazione con il traffico esistente sui collegamenti principali da parte dei servizi, deve essere calcolato in anticipo per garantire correttamente una trasmissione fluida e affidabile.

La parte fondamentale dell'installazione è alimentata da PoE con un consumo energetico che dipende da diversi fattori, come il tipo di telecamera e gli accessori (riscaldatore, motori, ecc.). Nella fase di progettazione della rete, gli switch di accesso collegati alle telecamere IP devono essere scelti in modo da poter fornire l'alimentazione sufficiente a gestire tutte le telecamere collegate.

Supporto ONVIF

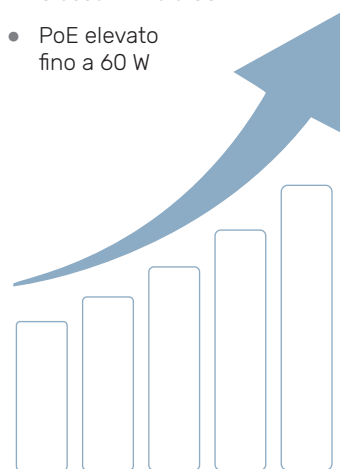
Allied Telesis ha semplificato l'installazione e la configurazione delle reti di videosorveglianza aggiungendo il supporto per i protocolli ONVIF alla sua soluzione di automazione di rete AMF Plus. Ciò consente di semplificare l'installazione, la gestione e la manutenzione delle telecamere di sicurezza remote.

Integrazione delle pietre miliari

Il plug-in di integrazione Milestone è un componente aggiuntivo del VMS XProtect di Milestone System che consente il controllo diretto delle telecamere IP collegate agli switch Allied Telesis. Il plug-in semplifica la gestione remota delle telecamere per il personale di sicurezza, integrando le comuni attività di amministrazione nell'interfaccia grafica di XProtect, risparmiando tempo e costose chiamate.

Classe PoE

- Classe 0 fino a 15 W
- Classe 1 fino a 4 W
- Classe 2 fino a 7 W
- Classe 3 fino a 15 W
- Classe 4 fino a 30 W
- PoE elevato fino a 60 W



INFORMAZIONI SU ALLIED TELESIS

Da oltre 30 anni, Allied Telesis fornisce connettività affidabile e intelligente per tutte le esigenze, dalle organizzazioni aziendali ai progetti di infrastrutture critiche e complesse in tutto il mondo.

In un mondo che si muove verso le Smart City e l'Internet of Things, le reti devono evolversi rapidamente per affrontare le nuove sfide. Le tecnologie intelligenti di Allied Telesis, come Allied Telesis Autonomous Management Framework™ Plus (AMF Plus) e Enterprise SDN, garantiscono che l'evoluzione della rete possa tenere il passo e fornire soluzioni efficienti e sicure per le persone, le organizzazioni e le "cose", sia ora che in futuro.

Allied Telesis è riconosciuta per aver innovato il modo in cui vengono forniti e gestiti servizi e applicazioni, con conseguente aumento del valore e riduzione dei costi operativi.

Visitateci online su alliedtelesis.com.

