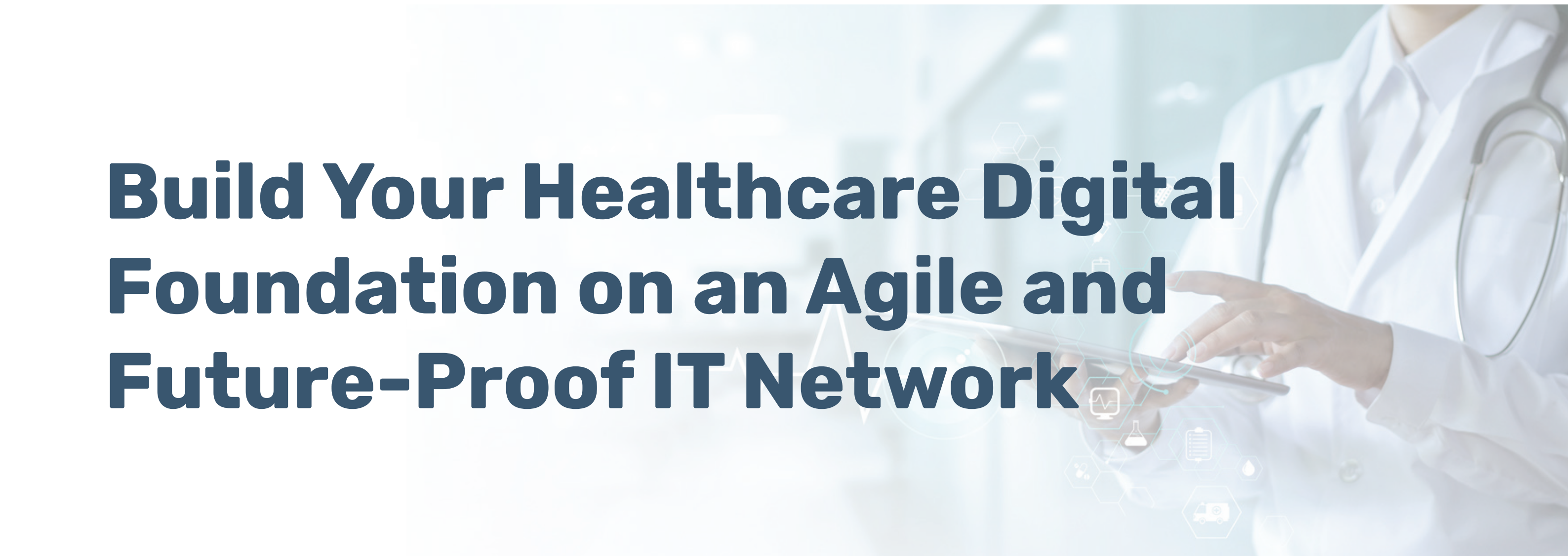
WHITE PAPER | September 2020

Allied Telesis



Build Your Healthcare Digital Foundation on an Agile and Future-Proof IT Network

The healthcare industry is undergoing a rapid pace of change, making digital transformation a business imperative. The global pandemic has accelerated innovation, putting even more pressure on IT networks to adapt to heightened needs. As connected care continues to grow, Allied Telesis networking ensures that facilities can deliver the most secure and reliable solutions to the people in their care.

Introduction

Even before the global coronavirus pandemic hit the healthcare industry like a nuclear bomb, there were significant business changes and technology upheavals taking place. On the business side, rapidly rising medical costs, a shortage of skilled healthcare workers, disappearing rural services, a new emphasis on personalized care, and other factors have been driving changes in how healthcare is delivered to patients.

On the technology side, the capabilities of legacy IT networks are strained by the adoption of mobile and remote care, the need for secure real-time access to electronic health records (EHR), an explosion of connected medical devices, the migration of sensitive data and applications to the cloud, and the use of advanced AI-based technologies to develop customized care.

Now and in the years ahead, healthcare IT leaders need to address a wide range of both business and technology challenges and opportunities.

The wide-area network (WAN) underpins nearly everything that takes place in hospital or clinical facilities as well as at many offsite locations, including ambulatory services and patients' own homes. A top consideration is how to build a solid yet agile network that can support all the current needs and which futureproofs the organization as new needs emerge.

Global healthcare systems vary greatly from country to country, region to region. Some systems are government driven, while others are privately-owned enterprises. Nevertheless, they have a lot in common—most notably the responsibility to deliver

the highest quality care at the lowest possible cost. Technology plays a huge role in how that mission can be accomplished.

This document looks at the drivers for change in healthcare, priorities for healthcare IT networks, what's needed to build such networks to ensure they are agile and ready for the future, and how Allied Telesis meets those needs with robust networking and security solutions.

Major Drivers for Change in Healthcare

Long before the coronavirus completely upended the global healthcare industry, significant changes were already taking root. Every healthcare organization is looking for ways to provide patient care with better outcomes, to become more operationally efficient, and to lower or at least contain the cost of delivering care. Organizations are using the drivers listed below to reach those business objectives.

Electronic Health Records (EHRs)

HealthIT.gov defines an electronic health record as a digital version of a patient's paper chart. EHRs are real-time, patient-centered records that make information available instantly and securely to a variety of authorized users.

There has been a worldwide move toward EHRs for more than a decade. Some countries, such as the U.S., mandated adoption years ago and are fully implemented, or nearly so, today. Other countries are just beginning their journey to digitize patients' medical records.

Full implementation of EHRs is necessary to automate and streamline provider workflow and to share essential information about a patient's medical history with a range of providers across multiple healthcare organizations. Not only doctors and nurses but also laboratories, pharmacies, specialists and other clinicians involved in a patient's care can be authorized to access the real-time data.

The IT Implications of EHRs

Digitized medical records are often stored in the cloud, where they can be made available to a wider base of authorized users. Real-time access to EHRs is necessary for providers to deliver accurate and timely care. EHRs may contain large image files, like those for x-rays and MRIs. Thus, high-speed, high-bandwidth network connections are needed to access and transmit the records.

Security of the EHRs is of highest importance, given the sensitive nature of the personal information. What's more, this data is of high appeal to hackers. Patient records can sell for up to $1,000 due to the amount of information found in the documents, including date of birth, credit card information, social security number, insurance information, home address and email address[1]. Hackers can turn around and use this data for medical fraud and other nefarious purposes.

Telehealth/Remote Care

The Health Resources Services Administration defines telehealth as the use of electronic information and telecommunications technologies to support long-distance clinical health care, patient and professional health-related education, public health, and health administration.

An even broader trend beyond that definition of telehealth is remote patient care, which includes home hospitalization. In this form of remote care, a patient who might normally have a lengthy stay in a hospital is discharged early to finish the rest of the hospital care at home. The patient has a medical team monitoring his conditions around the clock and making in-person visits daily.

The coronavirus pandemic has pushed many healthcare organizations to accelerate adoption of different forms of telehealth or remote care. Frost & Sullivan forecasts a seven-fold growth in telehealth In the United States by 2025—a five-year compound annual growth rate of 38.2%[2]. In the U.S. in particular, telehealth is compensating for the loss of rural hospitals and clinics. In countries such as Italy, England and Australia, home hospitalization has been offered for years to reduce healthcare costs and reserve actual hospital beds for the sickest of patients. Studies show that programs like these provide better outcomes for patients[3].

The IT Implications of Telehealth and Remote Care

Technologies commonly used for telehealth and remote care solutions often include audio and video conferencing, digital cameras and scopes, mobile and fixed-line broadband, store-and-forward imaging, data monitoring, smart phone apps, streaming media, mobile diagnostics, terrestrial and wireless communications, and a range of mobile medical devices.

Obviously, consistent and reliable broadband connectivity between patient and provider is critical to smoothly transmit the audio/video/images/data. In addition, the connections must be 100% secure to prevent theft of sensitive data.

The Internet of Medical Things (IoMT)

The Internet of Medical Things is comprised of a burgeoning range of connected medical devices that are used to perform diagnostics, monitor a patient's condition, automatically administer medications, and perform many other essential care-related tasks. Even hospital beds today are considered "smart" as their sensors record the patient's movements and monitor his status.

The average hospital room contains 15-20 connected medical devices, and sometimes even more. In some hospitals, connected medical devices outnumber laptops and smartphones, 4 to 1. A large hospital could be home to as many as 85,000 connected devices[4].

The IT Implications of the IoMT

Support for a large number of simultaneous connections is vital. Such demands dictate a need for a robust network with high capacity bandwidth. Moreover, many of these medical devices can be moved from room to room, making continuous wireless connectivity an essential element of their operation. For example, as a patient is moved from his private room to a diagnostic room where an MRI will be administered, various monitoring devices may need to move with him and maintain a continuous connection to the network.

Security is an important aspect of these IoMT devices. They must authenticate themselves to the network to obtain access, ensuring that no one can plug in an unauthorized device and easily get access to the network.

Other Important Drivers for Change in Healthcare

There are other drivers that have an impact on IT networking in healthcare organizations. For instance, there's a vast shortage of skilled workers in both nursing and information technology. This is leading healthcare organizations to look toward automation and other means to compensate for the dearth of workers.

Consolidation is taking place throughout the healthcare industry as independent hospitals and practices are acquired by larger organizations. As with any M&A activity, the acquiring organization is looking for economies of scale to better compete in its marketplace.

The cost of delivering healthcare services is rising rapidly. Global healthcare spending is expected

to rise at a CAGR of 5% in 2019-2023[5]. In many European countries, healthcare expenditures have reached or exceed 10% of GDP[6]. In the U.S., the figure is much higher and is projected to become nearly 20% of GDP by 2027[7]. Organizations are looking for viable means to address the sharp rise in costs.

And of course, the global pandemic is having a huge impact on the way healthcare organizations operate today, and many new processes will become a permanent way of work. Ironically, as Covid-19 patients fill hospital wards, many of those same hospitals are having to furlough medical staff who have been sidelined during the pandemic. The elective services they offer are being delayed or canceled, which reduces revenue overall for the hospital and clinicians. Where possible, telehealth and home hospitalization are offered as alternatives for in-person care. In general, the pandemic is accelerating the use of technology in all forms in healthcare.

General Requirements for Healthcare IT Networks

IT networks in hospital and clinical environments obviously have a lot of demands on them—to support the drivers discussed above as well as other needs. Networks are challenged to run faultlessly, 24 hours a day, every day. More so than regular office environment networks, healthcare IT networks must be exceptionally reliable, must support simultaneous connectivity for a large number of disparate devices, and must enable real-time access to critical and highly sensitive data for authorized users only. What's more, IT networks must be easy to administer and manage, and must be adaptable enough to support unknown future needs.

In broad terms, here are the general requirements for healthcare IT networks:

Provide consistent connectivity to a highly reliable wide area network

From connected medical devices to mobile access to electronic health records, and everything in between, virtually every aspect of the healthcare industry today is dependent on a mission-critical IT network that is continuously available to the authorized people and devices that need to connect to it. Whether these entities are in the same building, across a campus, or across a region, consistent connectivity to a highly reliable network is fundamental. Large organizations need support and optimization for multi-site WAN connections as well as remote access.

Given the high level of mobility in healthcare today, connectivity must be delivered via both wired routers and switches and wireless access points. Special attention must be given to the wireless networking to avoid conflicting signals, dead spots, and dropped connections as caregivers and medical devices move from room to room throughout the facility.

In many healthcare markets, telehealth and home hospitalization programs require not only technology at the remote point of care, but also reliable, secure and high bandwidth connectivity between caregiver and patient.

Provide secure network access for authorized people and medical devices

Authorized care providers and medical staff need secure access to the network and the data it harbors, regardless of where they are or what device they are using. Patients and family members need segmented guest access to the Internet and patient entertainment systems. Medical devices need their authorization to gain secure access to the network in order to send and

receive data and to be monitored to ensure their consistent performance. In all cases, secure access should be based on the identity and context of each entity and not simply based on IP address.

Protect highly sensitive patient data

Data protection is paramount. Healthcare providers around the world are under government regulations to protect the privacy of confidential patient data from unauthorized access. Much of this data today is digitized, or soon will be, and quite often it is stored in the cloud for broader access. Effective security measures include layers of security, both at the network perimeter as well as directly around the data and workloads, wherever they reside.

Be easy to administer and manage

A healthcare network must be easy to configure, deploy, manage, and troubleshoot—thus minimizing costly administration and downtime. There must be clear visibility of network traffic in order to optimize both network performance and operational costs. The network must support centralized management for branches as well as remote sites without IT resources. Automation in network management is a must; for example, to maintain uptime through automatic recovery from equipment or link failure.

Be ready for the future

Networking technologies and architectures are undergoing rapid change these days. Enterprises are shifting from traditional WANs that make an on-premise datacenter the center of the network universe, to agile, software-defined WANs that can easily serve branch locations, mobile and remote users, and cloud-based applications and workloads. A healthcare IT network must be "software-defined" to support new and emerging business applications, a vast and increasing array of connected medical devices, "healthcare without walls" that expands beyond the hospital or clinic to serve people where they are, and whatever else the future may bring.

> "Allied Telesis has a very good basic infrastructure for networking, and that is what our healthcare customers need. They need a robust networking solution in both the wired and Wi-Fi networks and strong security in the firewall systems. We recommend Allied Telesis most often to our customers because of the simple but clever administration tool to administer all the devices. AMF provides for centralized administration with automation that makes it simple to control hundreds of thousands of switching ports. This is one of our customers' biggest needs, and Allied Telesis really delivers."
>
> – Siegmund Gromotka, Geschäftsführer bei (CEO) inducio GmBH

The Allied Telesis Solution for Healthcare

Unstoppable Network Access

Integrated healthcare systems require uninterrupted communication among different hospitals and remote clinics, facilities and even patients' homes. High availability and accessibility of the IT infrastructure are vital for the whole healthcare ecosystem.

There is much riding on the core network of any healthcare organization. The Allied Telesis unstoppable network access solution ensures that the network is able to survive multiple faults while still maintaining connectivity in a wide range of network architectures, thus providing a highly available solution.

Allied Telesis considers multiple factors in building the unstoppable network.

Network Equipment Power Supply: Allied Telesis uses a series of equipment with a redundant power supply system to ensure that the network remains fully operational in the event of an internal power failure.

Simplified Network Device Power Supply: Many devices in hospitals are connected directly to network switches. The use of Power over Ethernet-enabled equipment to power these devices enables backup power provisioning to the switch and delivers power back to the attached devices.

Virtual Stacking: Multiple Allied Telesis switches can be connected to form a single virtual switch. Together, the Virtual Chassis Stacking technology with Link Aggregation provides a resilient solution that is able to survive a link or equipment failure.

Ring Protection: When the distance between devices is large, a ring topology is the optimal solution for the network. Allied Telesis provides Ring Protection protocols to save the network from link failure while providing a resilient infrastructure.

Redundant Core and Disaster Recovery: For a further degree of resiliency, Allied Telesis also can provide core switches with an optimally redundant configuration for a disaster recovery architecture. This is accomplished by a virtual stack with network devices located in different rooms or buildings.

Reliable and Easy WAN Management

The patient-centered approach of the healthcare industry follows the direction of service decentralization, where care facilities are located remotely from the hospital. These sites need to be connected to the main network as if they were in the same hospital building with secure and reliable access.

To provide high availability service to these remote sites, the recommendation is to connect the sites using multiple links and to split the traffic between them depending on the application, the link cost, and other considerations. The use of multiple links permits a backup in case of line failure and results in a high availability solution.

Allied Telesis Software-Defined Wide Area Network (SD-WAN) management simplifies remote site connection management with an autonomous and centralized management tool. This SD-WAN orchestrator centrally manages remote facility connections for reliable and secure application delivery. This tool is used to set acceptable performance metrics, automatically optimize and load-balance application delivery, and easily monitor WAN performance. In addition, SD-WAN paired with Allied Telesis application-aware firewalls provides an integrated WAN security and WAN traffic management solution in a single device.

No Compromise Wi-Fi

In addition to medical staff carrying mobile devices from room to room, a large number of medical devices such as image diagnostic and wearable monitors require a stable wireless network to provide or to access information in real time. For security reasons, devices with access to patient data require the user to reauthenticate once the network connection drops. For this reason, Allied Telesis delivers an uninterrupted roaming-free wireless solution for the healthcare market. A wireless connection is also used by medical devices as a backup link in case the wired connection fails, thus adding reliability to the whole network solution.

Allied Telesis has unique, industry-leading technology to ensure reliable wireless connectivity. Client disconnection and slow communication are common wireless problems usually caused by one or more technical issues. Interferences between radio channels, external wireless sources not under IT control, and access points' signal strength are the main reasons for wireless problems. Moreover, highly skilled people are often needed to resolve these problems.

Allied Telesis technology overcomes those issues with the No Compromise Wi-Fi solution. It ensures reliable, high performance wireless connections everywhere they are needed without increasing the need for skilled IT resources.

By analyzing signal coverage gaps and Wi-Fi Access Point interference, Autonomous Wave Control (AWC) automatically delivers a high-quality wireless experience. This allows a hospital to reduce its dependency on skilled network engineers and enjoy lower operating costs. AWC Channel Blanket (AWC-CB) enables control of hybrid Access Points that simultaneously provide single and multi-channel Wi-Fi connectivity. Channel Blanket is the best radio technology to provide a seamless connection to critical personal and medical devices as they move around the hospital.
AWC-CB also enables device location tracking to easily find equipment and reduce losses of expensive equipment.

Network Management Made Easy

As networks grow more complex, the demands on network management and specialized IT resources grow significantly. Allied Telesis recommends implementing an automation solution to simplify and lower the cost of managing the network.

Vista Manager EX is a plug-in based single-pane-of-glass approach to network management. It has a dashboard showing network details, status, and events on a topology map, and it highlights critical issues to minimize reaction time and to help resolve problems in a timely fashion. A series of plugins to control the wired network, wireless devices, the WAN link and automation tools make networking easy and the solution modular.

Autonomous Management Framework (AMF): Hospitals can reduce network operating costs with the added intelligence and automation of centralized management. AMF is an intuitive solution for many network topologies. It can be overlaid on existing network infrastructure to reduce new equipment costs. What's more, the automation of network management tasks leads to reduction in costs and maintenance and support.

Automated services including firmware upgrades, backup, recovery, and zero-touch provisioning are among many AMF benefits to minimize the resources and skills required to manage a complex healthcare network. As a scalable network management platform, AMF supports Allied Telesis switching, firewall, and wireless products, as well as a wide range of third-party devices.

Autonomous Wave Control (AWC) plugin: This tool enables hospitals to analyze and optimize the performance of complex wireless networks. They can install and forget the wireless network with an autonomous tool that analyzes traffic patterns and automatically configures access points to meet demand.

Software-Defined WAN (SD-WAN): Hospitals can centrally manage and automatically optimize inter-branch traffic with the SD-WAN plugin.

Simple Network Management Protocol (SNMP) plugin: This tool enables auto discovery and management of a wide range of devices in a multivendor environment within Vista Manager EX.

Security and the Self-Defending Network

Cyber-attacks on medical institutions are on the rise and becoming more frequent. Unauthorized access to patient data, ransomware and other types of attacks affect the daily operations and result in serious risk to patient privacy.

The traditional security models that focus on preventing attacks from getting inside the network are not enough since attacks can easily come from within. For example, an infected tablet or IoMT device connected to the network can pose a serious threat. In parallel, attackers have increased the sophistication in their methods and now threats come in so many forms that maintaining a secure effective network has become a time-consuming and costly challenge.

While the traditional firewall-based approach is effective to detect and block threats and viruses coming from the Internet, it shows its limitations if the attack comes from inside the network. Thus, Allied Telesis has devised the Self-Defending Network solution to provide an integrated approach to network security, automating manual IT operations and protecting from threats coming from both wired and wireless access devices. Without the need for endpoint agents or software, the Self-Defending Network is able to automatically respond to threats once they are identified.

The Allied Telesis AMF-Sec Controller is a software service that enables state-of-the-art network management and security. It provides exactly what healthcare organizations need—reduced management costs, increased security, and an improved end-user experience.

Firewall and security appliances identify threats, and then the intelligent engine implementing the Isolation Adapter technology built into the AMF-Sec Controller responds immediately to isolate the affected part of the network and quarantine the suspect device. Remediation can be applied so the device can rejoin the network with minimal disruption. Responses are configurable, and comprehensive logging provides a clear audit trail.

AMF-Sec is OpenFlow v1.3 compatible and suitable for both wired and wireless networks. It integrates with business applications to save time and money, and with security products to detect threats. It is scalable so that more business apps can be added for greater value.

Network security must also consider the firewall architecture. Allied Telesis recommends a firewall between the LAN and WAN, firewall offloading to support high performance, and network segmentation with a local firewall between the network segments to minimize the spread of local viruses (e.g., from administrative offices to Medical Image analysis) and to preserve the most important part of the network (e.g., Operating Room or Patient Data Monitoring).

Conclusion

Healthcare organizations are under extreme pressure today, and their IT networks must be able to adapt to new ways of work. Networks must be agile to address today's challenges, intelligently automated to reduce the burden on technical staffs that are stretched thin, and software-defined in order to be ready for future needs. Allied Telesis provides robust networking solutions that are the perfect prescription for healthcare IT networks, today and tomorrow.

To learn more about Allied Telesis offerings for the healthcare industry, please visit https://www.alliedtelesis.com/en/solutions/industry/healthcare.

About Allied Telesis

With a portfolio of products and technologies providing IoT and SDN-enabled solutions for enterprise, government, education and critical infrastructure customers, Allied Telesis is the smarter choice. Its Envigilant™ managed services division delivers customized, state-of-the-art IoT solutions at the edge, empowering innovation, improving process agility, and helping build a competitive advantage for customers globally.

We are committed to providing our customers with solutions designed and built to the highest standards and quality. Our manufacturing conforms to ISO 9001 standards and all of our facilities adhere to the strict ISO 14001 standard to ensure a healthier planet.

For more information, visit https://www.alliedtelesis.com/.

[1] Mackenzie Garrity, Patient medical records sell for $1K on dark web, February 20, 2019

[2] Frost & Sullivan, Telehealth to Experience Massive Growth with COVID-19 Pandemic, Says Frost & Sullivan, May 13, 2020

[3] Abigail Abrams, Time magazine, "New technology expands access, turning patients' bedrooms into 'hospitals'," August 2020

[4] Elizabeth O'Dowd, "Considerations for Connected Medical Device Networks," HIT Infrastructure, July 7, 2017

[5] Deloitte, 2020 Global Health Care Outlook

[6] Eurostat, Healthcare Expenditure Statistics, April 2020

[7] Peter G. Peterson Foundation, "Healthcare Costs for Americans Projected to Grow at an Alarmingly High Rate, May 2019