BUSINESS PAPER

aruba
a Hewlett Packard Enterprise company

SD-WAN for Healthcare

HOW SD-WAN HELPS HEALTHCARE ORGANIZATIONS EMBRACE DIGITAL TRANSFORMATION

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The pandemic crisis has highlighted the need to transform healthcare, reduce inequalities in access to medical care, and provide a more personalized and humane experience. Patients and caregivers have recognized the convenience and effectiveness of telehealth during the crisis. In addition, the health sector is accelerating the digitalization of its services and transforming its hospitals into smart hospitals. Medical records are now stored electronically, and the sector is using an increasing number of IoT devices, which are inherently unsecure. However, this transformation exposes healthcare providers to significant data breaches and growing cybersecurity risks while they must demonstrate compliance to standards that protect sensitive health information such as HIPAA.

In this context, a traditional MPLS router-based network architecture is no longer sustainable. It is often rigid, complex, and provides a poor quality of experience.

This paper examines five use cases in the healthcare sector that demonstrate how an advanced, secure SD-WAN solution helps healthcare organizations streamline digital transformation efforts, improve security, and accelerate compliance. These use cases include:

- **Rapidly and reliably connect remote medical sites**
- **Move to a cloud-first model and implement SASE**
- **Deliver the best telemedicine experience**
- **Improve security of Electronic Medical Records and IoT devices with a zero-trust network**
- **Comply to HIPAA mandates: Delivering privacy and security for ePHI with a business-driven SD-WAN**

CHALLENGES IN THE HEALTHCARE SECTOR

The COVID-19 crisis has highlighted some gaps in the health sector in various domains. It has indeed revealed inherent problems such as unequal access to care, the lack of intensive care beds in hospitals, and the shortage of health workers.

The crisis has demonstrated the need for a more equitable approach to healthcare and for providing high quality, affordable health care, as some communities have been more affected by the pandemic than others. A recent Boston Consulting Group report[1] mentions that "The COVID-19 death rate in the US among black people is more than twice that of whites, and more than 85% of the difference is attributable to greater risk exposure and less access to testing."

Reinventing healthcare

As the pandemic placed public health systems under increased pressure, it illuminated the need for more efficiency and prevention from the governments. Countries that rely on public health systems have started to create initiatives to overhaul their healthcare systems. According to a Deloitte study[2], Japanese citizens will be able to access their personal health records (PHR) online, including test results and medical history. The German government has funded several projects that include patient portals, digital medication management, telemedicine, and robotics.

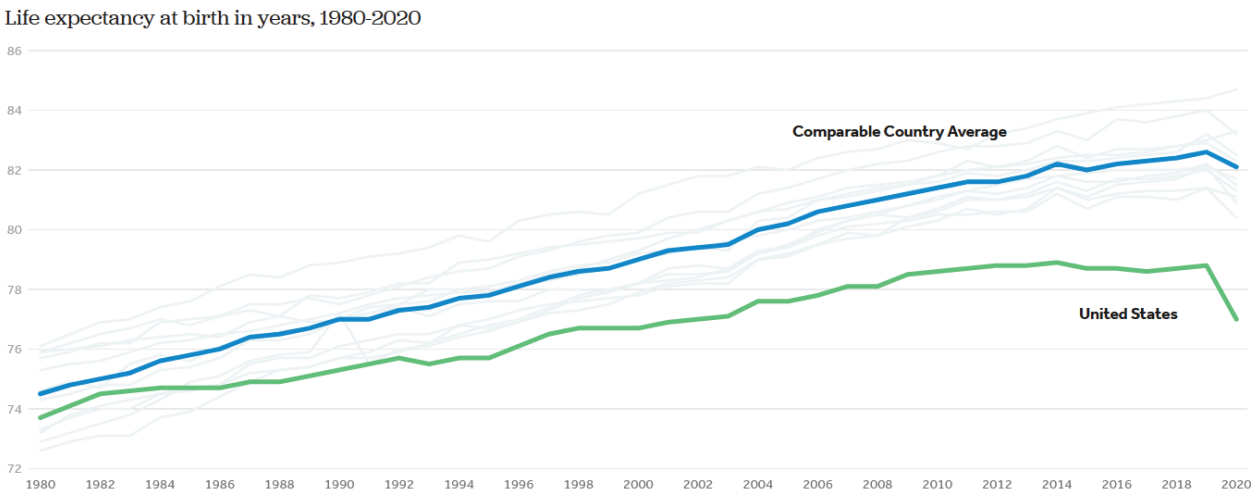
The COVID-19 crisis has also had serious repercussions on mental health, such as depression or anxiety disorders. There's now an emerging idea that healthcare is not only about hospitals and doctors but must become more socially responsible. According to the same study, "social, economic, and environmental drivers of health can account for up to 80% of health outcomes, whether positive or negative. These drivers of health include factors such as income, location of residence, and the quality of social support networks".

While in most developed countries life expectancy has steadily increased, it has decreased in the recent years in the US despite higher spending. The decrease is not solely due to the COVID crisis, but also it is due to social factors like the opioid crisis, the obesity rate, and homicides.

To address these challenges, governments must go beyond traditional health care and implement integrated approaches to public health policies, housing, education, transportation, and employment, to better coordinate health care needs geographically. New levels of collaboration between governments, insurance companies, healthcare industry and local communities must be developed. Health disparities must be reduced with healthcare providers working closer with their patients.

[1] Source: Health Care's New Reality Is Dynamic, Digital—and Here to Stay, Boston Consulting Group, Dec. 2021

[2] Source: 2022 Global Health Care Outlook, Deloitte, 2021



Life expectancy has steadily declined in the US in the last decade compared to similar countries
Source: KFF Analysis of CDC, Australian Bureau of Statistics and OECD data

The health sector must work on providing a personalized, convenient, and more approachable experience. Consumers are indeed looking for more convenience as shown by a McKinsey study[3] with more than 60 percent of consumers expecting to be able to change or schedule a healthcare appointment online. At the same time, home-care capabilities, such as home-based dialysis, primary home care, and hospital-at-home models—are growing rapidly to provide a more convenient approach according to the same study.

The shift to lower acuity settings instead of hospital stays is also confirmed by a BCG study[4] that found that 60% of patients are willing to transition from hospital-level care, 52% are willing to transition from hospital-associated clinics, and 32% are willing to go to whatever site their physician recommends for care. The ambulatory care segment also increases as it provides many advantages such as shorter visit length and lower complications.

Patients state a preference for care in lower-acuity settings

New site of care preference (%) →

Original site of care	Hospital	Off-hospital clinic/office associated with a hospital	Independent clinic/office	Wherever my doctor recommends	
Hospital	40	24	9	28	**=60%** Willing to step down from hospital-level care
Off-hospital clinic/office associated with a hospital	7	41	22	29	**=52%** willing to step down from hospital-associated clinic
Independent clinic/office	3	9	55	32	**=32%** willing to return wherever is recommended

Source: BCG patient sentiment survey, May 2020.

[3] Source: The next frontier of care delivery in health care, McKinsey, March 2022

[4] Source: Health Care's New Reality is Dynamic, Digital – and Here to Stay, Boston Consulting Group, Dec. 2021

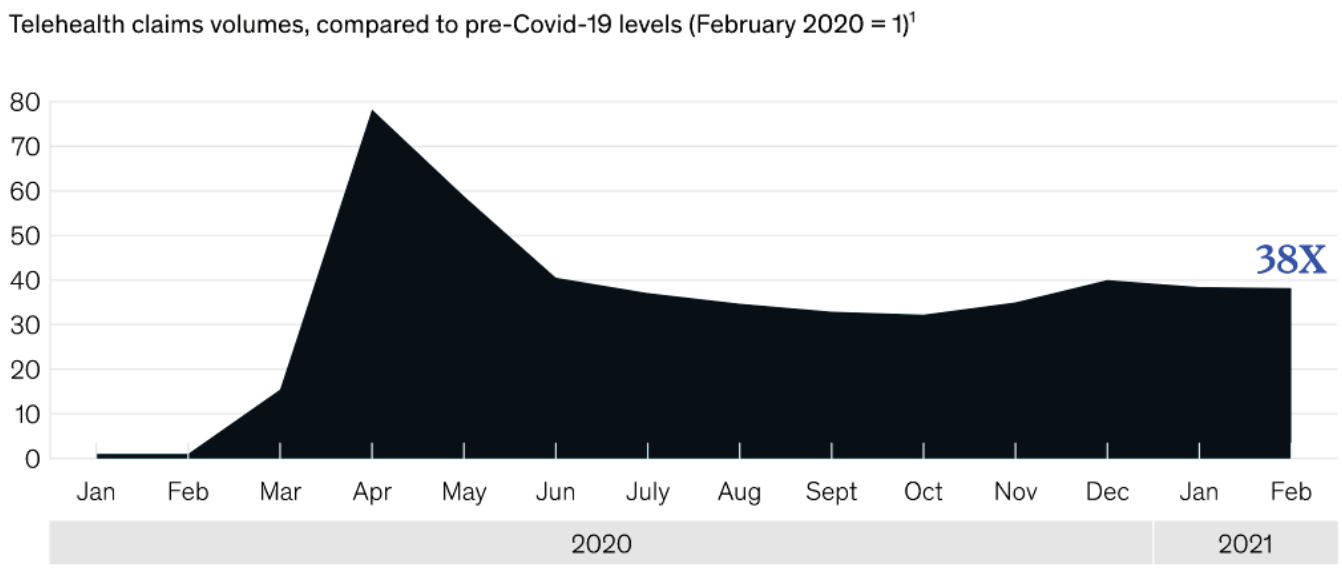
In that context the digitization of the healthcare industry has become key to enable new healthcare delivery models including telehealth, smart hospitals, and the digitization of public health systems. However, the digitization of the health sector poses new threats of cybersecurity and data privacy as we'll see in the next paragraphs.

The digitization of the health sector and telehealth

Telehealth is now here to stay as it has proven to be an efficient way to replace on-site consultations and has become popular with both patients and care providers. Additionally, regulatory changes implemented by governments allow for greater access and reimbursement of telehealth.

A McKinsey study[5] shows that telehealth utilization has stabilized at levels 38 times higher than before the pandemic. The study also reveals that 76% of consumers are "highly or moderately likely" to use telehealth in the future.

Growth in telehealth usage peaked during April 2020 but has since stabilized



[1] Includes cardiology, dental/oral, dermatology, endocrinology, ENT medicine, gastroenterology, general medicine, general surgery, gynecology, hematology, infectious diseases, neonatal, nephrology, neurological medicine, neurosurgery, oncology, ophthalmology, orthopedic surgery, poisoning/drug tox./comp. of TX, psychiatry, pulmonary medicine, rheumatology, substance use disorder treatment, urology. Also includes only evaluation and management visits; excludes emergency department, hospital inpatient, and physiatry inpatient claims; excludes certain low-volume specialties.
Source: Compile database; McKinsey analysis

Source: Telehealth: A quarter-trillion-dollar post-COVID-19 reality? McKinsey, July 2021

In the same BCG study, two-thirds of providers believe that the use of virtual consultations will accelerate over the next one to three years. More than 30% of providers say that patients' use of digital and diagnostic tools is common now, compared with only 17% that held this view before the pandemic.

According to this study, many medical activities such as test results reviews and primary care are now preferably performed online. Healthcare providers that don't provide telehealth services are more susceptible to lose patients.

[5] Source: Telehealth: A quarter-trillion-dollar post-COVID-19 reality?, McKinsey, July 2021

What percentage of interactions with patients will be conducted virtually in 3-5 years? (%)

	First interaction/visit	Test results review	Pre-operation visits	Direct postop followup	Long-term followup continuing care	Overall Average
Cardiology	33	65	34	34	58	45
General surgery	31	62	36	35	59	45
Dermatology	46	63	46	48	60	53
Oncology	27	53	30	30	48	37
OB/GYN	28	60	31	37	53	42
Primary care	53	69	48	51	67	58
Overall average	36	62	37	39	57	

60%-69%
50%-59%
40%-49%
30%-39%
20%-29%

Test results review and primary care are now preferably performed online, source: BCG health care executive survey, August 2021

The shift to "smart hospitals" has also accelerated to improve quality and efficiency. In addition to telehealth, it includes artificial intelligence (AI), robotics, 3-D printing, augmented reality/virtual reality, IoT sensors, and enhanced digital imaging capabilities like PACS (picture archiving and communication system) to securely store and digitally transmit electronic images such as X-rays and MRIs.

The number of IoT devices and their applications in the healthcare sector are growing exponentially. According to Gartner[6], IoT spend by healthcare providers will grow from $16 billion in 2018 to nearly $52 billion in 2028 at a compound annual growth rate of 12%. IoT devices in healthcare support a vast array of applications including patient monitoring, ingestible sensors, in-home care, smart hospital equipment, and medical supplies inventory. The benefits of IoT in the healthcare sector are gigantic helping accelerate diagnosis, improve patient care, and reduce errors.

This shift to smart hospitals translates into more networking bandwidth to transmit large amounts of digital images like MRI and PACS files, and telemedicine that requires high-quality videos, teleconferencing, and online communications.

Additionally, the healthcare sector is migrating their applications to the cloud, including patient management systems, electronic health record systems (EHR), and other business applications such as accounting. The need for more data storage in the cloud is also increasing to store an exponential number of digital images.

With most of the applications being hosted in the cloud, the data center is no longer the hub of all network connections. While many healthcare providers still rely on traditional network architecture using MPLS circuits to connect local healthcare facilities to the data center, this architecture is no longer adapted to cloud-first organizations. It indeed forces them to backhaul the traffic to the data center, impacting network performance and especially real-time applications such as video consultations.

Additionally, the increasing use of IoT devices raise many security issues as most of them are unprotected and are not able to run security agents. IoT is increasingly becoming a target for cyber attackers, and the risk is not only related to IT but also to patient health, that can potentially lead to dramatic incidents.

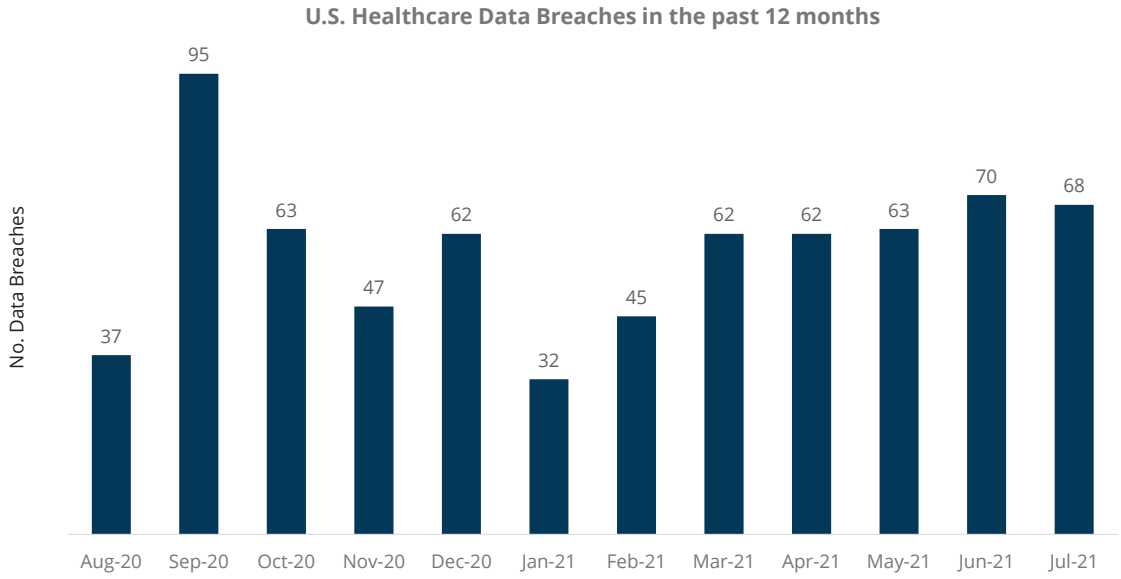
Cybersecurity and Compliance

As telehealth is widely used by patients and medical records are migrating to the cloud, data breaches are steadily increasing in the healthcare sector. The use of mobile devices for telehealth also makes medical data more vulnerable as most patients don't use secure networks or multi-factor authentication.

According to a recent study[7], the healthcare data of more than 44 million individuals has been exposed or compromised between August 2020 and July 2021 in the United States, and 706 healthcare data breaches have been reported.

[6] Source: Forecast Analysis: Healthcare Providers Internet of Things Endpoint Electronics and Communications Revenue, Worldwide, Gartner, Oct. 2019

[7] Source: July 2021 Healthcare data breach report, Hipaajournal.com, July 2021



Source: July 2021 Healthcare data breach report, **Hipaajournal.com, July 2021**

In addition, hospitals operate proprietary health record systems (EHR) that can even differ from one service to another. This incompatibility between health record systems duplicates sensitive data and increase potential attacks.

Ransomware is another major concern in the healthcare sector. In most cases, ransomware attacks consist of encrypting data or threatening hospitals to publish stolen data. In a 2020 survey[8], 34% of respondents mention they were hit by a ransomware attack, and 41% expect to be hit in the future. 34% of these organizations, admitted they paid the ransom to get back their data. The study also shows that the healthcare sector is more likely to pay the ransom compared to other sectors.

With 10 to 15 IoT devices per bed[9], IoT represents another threat. Many unmanaged devices can be found in healthcare environments such as infusion pumps, respirators, laboratory instruments, heart monitors, X-ray systems, and clinicians' handheld devices. These devices have limited – if not zero – security features. With the growing number of these devices in hospitals, the attack surface has significantly expanded, jeopardizing medical data security.

Legacy networks are no longer suited for today's sophisticated network security challenges. Furthermore, telehealth has created other vulnerabilities as patients can connect from anywhere outside of the healthcare security perimeter.

In healthcare, compliance is a key priority. If healthcare providers are not in compliance, it exposes them to several risks and hefty penalties. Increased cybersecurity risks have made compliance to security frameworks critical in this sector.

The Healthcare Insurance Portability and Accountability Act (HIPAA) is a US law passed in 1996 to modernize the flow of healthcare information, and protect patient information maintained by the healthcare and healthcare insurance industries from fraud and theft.

HIPAA mandates that healthcare providers implement IT security tools such as firewalls, intrusion detection, endpoint security, antivirus, and encryption controls to protect customer data. Also, it is critical to ensure that all third-party technologies used are secure and possess the HITRUST certification. HITRUST stands for the Health Information Trust Alliance. It provides a framework for organizations to show evidence of compliance with HIPAA-mandated security controls.

[8] Source: The State of Ransomware in Healthcare 2021, Sophos, 2021

[9] Source: HIPAA Journal, Sep. 2021

SD-WAN USE CASES SPECIFIC TO HEALTHCARE

Let's examine uses cases where healthcare organizations can accelerate digital transformation and move to a cloud-first organization by adopting an advanced SD-WAN platform.

Use Case #1: Rapidly and reliably connect remote medical sites

Healthcare facilities, hospitals, clinics, testing centers and imaging centers are geographically distributed and need a reliable connection to the headquarters and to the cloud.

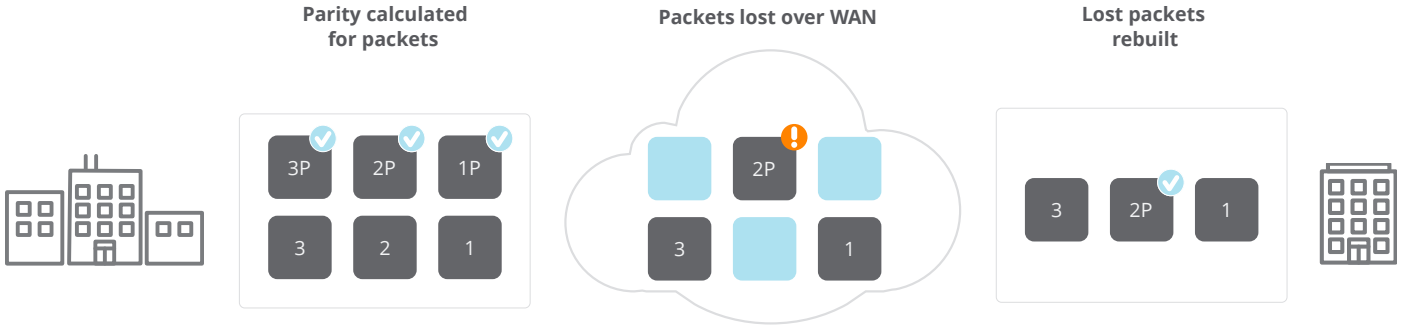
They often rely on MPLS connections to connect to the main data center, but these lines are expensive, they offer a limited bandwidth due to their costs and it often takes eight to twelve weeks to provision a new line preventing healthcare providers to quickly open a new facility.

On the other hand, broadband internet links are cheaper, easy to deploy, offer high network bandwidth, but they often suffer from jitter and packet loss affecting real-time applications such as VoIP and video conferencing. Remote sites may also experience latency due to their distance from the corporate data center.

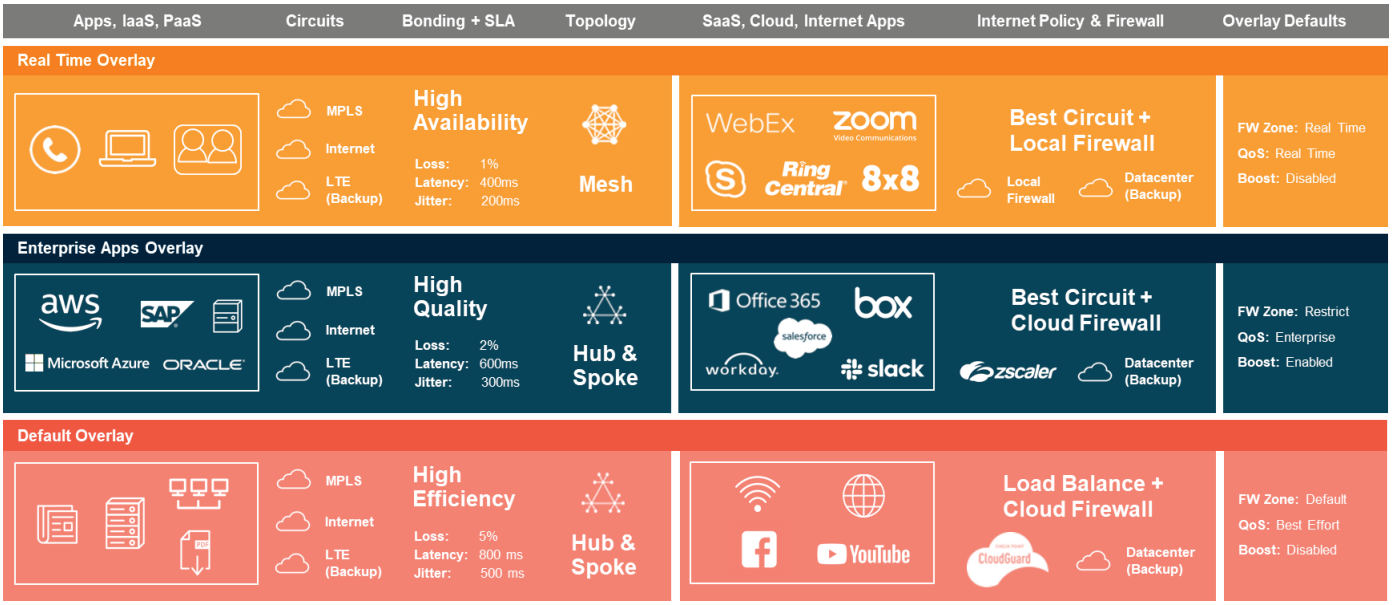
Through the virtualization of the WAN, Aruba EdgeConnect Enterprise SD-WAN is able to overcome internet and cellular network limitations by leveraging various features such as **Path Conditioning** and **Dynamic Path Control to make efficient use of all the available bandwidth**.

Path Conditioning: With an Aruba EdgeConnect Enterprise SD-WAN, healthcare providers can securely leverage internet broadband and 5G/LTE connections at a lower cost and obtain the same application performance - or even better - as when using dedicated private line services.

Path conditioning employs a **Forward Error Correction (FEC)** technology to detect and automatically reconstruct lost packets without having to retransmit them by sending periodic parity packets. In addition, **Packet Order Correction (POC)** re-orders any packets that arrive out of sequence at their destination. Path conditioning ensures a better user experience at these remote sites.



Forward Error Correction: packets lost in transmit across the WAN are automatically rebuilt



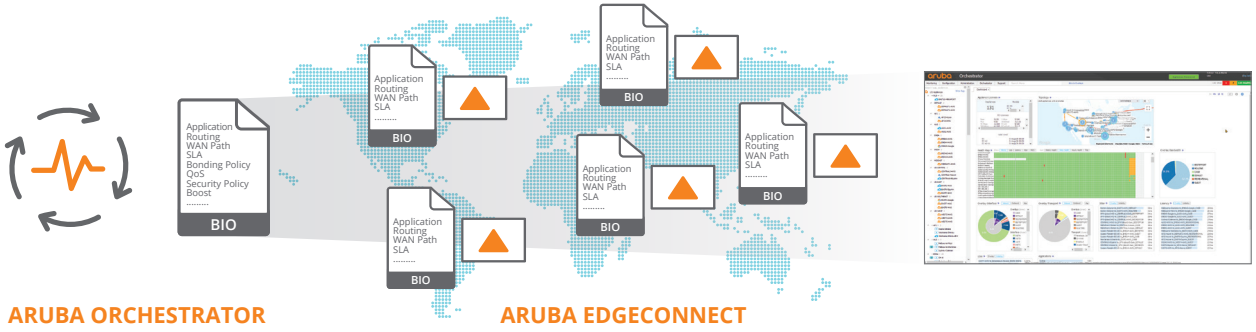
Business intent overlays enable healthcare providers to create virtual networks based on quality of service and business needs

Dynamic Path Control dynamically selects the best WAN transport(s) by continuously monitoring the throughput, packet loss, latency, jitter and MOS of all underlying WAN transport services. Aruba EdgeConnect Enterprise indeed combines multiple WAN transport services to create a single, higher bandwidth logical link. Link Bonding policies are configured in Business Intent Overlays and control how Aruba EdgeConnect Enterprise steers application traffic depending on business need and quality of service requirements.

By doing so, healthcare providers can augment an existing MPLS line with broadband internet, increasing reliability in case of brownouts and outages. **In some cases, MPLS connections can even be replaced by the reliable use of internet, satellite, or 4G/5G links and deliver a private line-like experience to remote sites**.

Aruba EdgeConnect **Zero-touch provisioning** greatly simplifies connecting and deploying a new site. A local office manager with limited IT experience can simply install an EdgeConnect SD-WAN appliance in a new remote site. The solution will self-register and once it has been authenticated, it will be admitted onto the SD-WAN fabric. Once authenticated, the solution automatically receives its configuration from Aruba WAN Orchestrator with no human intervention required at the location. Centralized orchestration also ensures that QoS and security policies are seamlessly enforced in remote sites.

Instead of taking months to deploy new sites, it takes a few days with an EdgeConnect SD-WAN while reducing costs and improving network efficiency.



Simplify and accelerate deployments with a top-down model and business-driven policies

Use Case #2: Move to a cloud-first organization and implement SASE

With the COVID crisis, healthcare providers have accelerated the move of their resources to the cloud including medical records, digital imaging databases, and business applications.

As more healthcare applications migrate to the cloud, it is no longer viable to backhaul the network traffic to the data center, seriously impacting application performance. It is critical to ensure a secure access to the cloud with sensitive data now in the cloud. Also, the growing use of off-the-shelf cloud applications such as Microsoft 365 or RingCentral, require routing traffic closer to the user to reduce latency and the hop count.

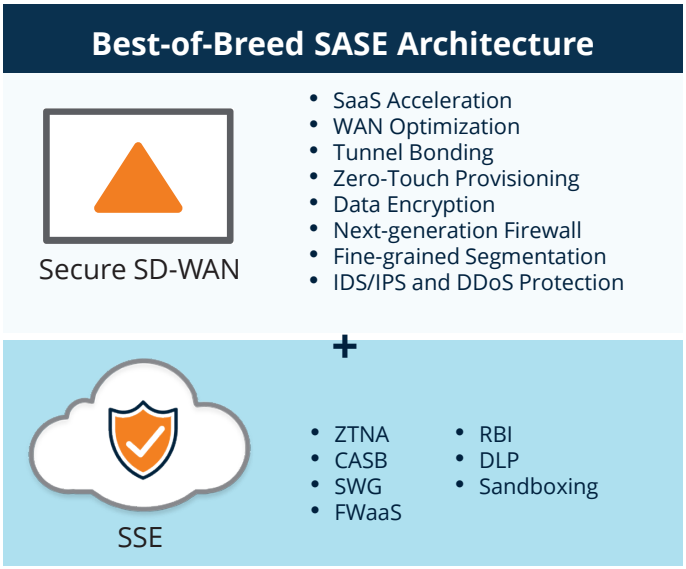
Aruba EdgeConnect Enterprise includes advanced features to support the move to the cloud and improve security such as local internet breakout and SaaS acceleration. It also supports a tight integration with a large number of cloud security vendors to implement a best-of-breed SASE architecture.

Local internet breakout: The EdgeConnect First-packet iQ™ feature identifies and classifies applications based on the first packet, enabling intelligent traffic steering to the internet according to business and security requirements. With this feature, trusted cloud application traffic, such as Microsoft 365 or UCaaS traffic, may be sent directly to the internet, while all other internet-bound traffic is sent to a cloud-delivered security solution for security inspection before it is handed off to the SaaS provider. In some cases, policies may dictate that the traffic be backhauled to the data center for advanced security inspection.

SaaS Acceleration: With this feature, Aruba EdgeConnect Enterprise improves SaaS application performance. It uses statistical learning to select the best path and the closest point of presence based on advanced network health and performance measurements.

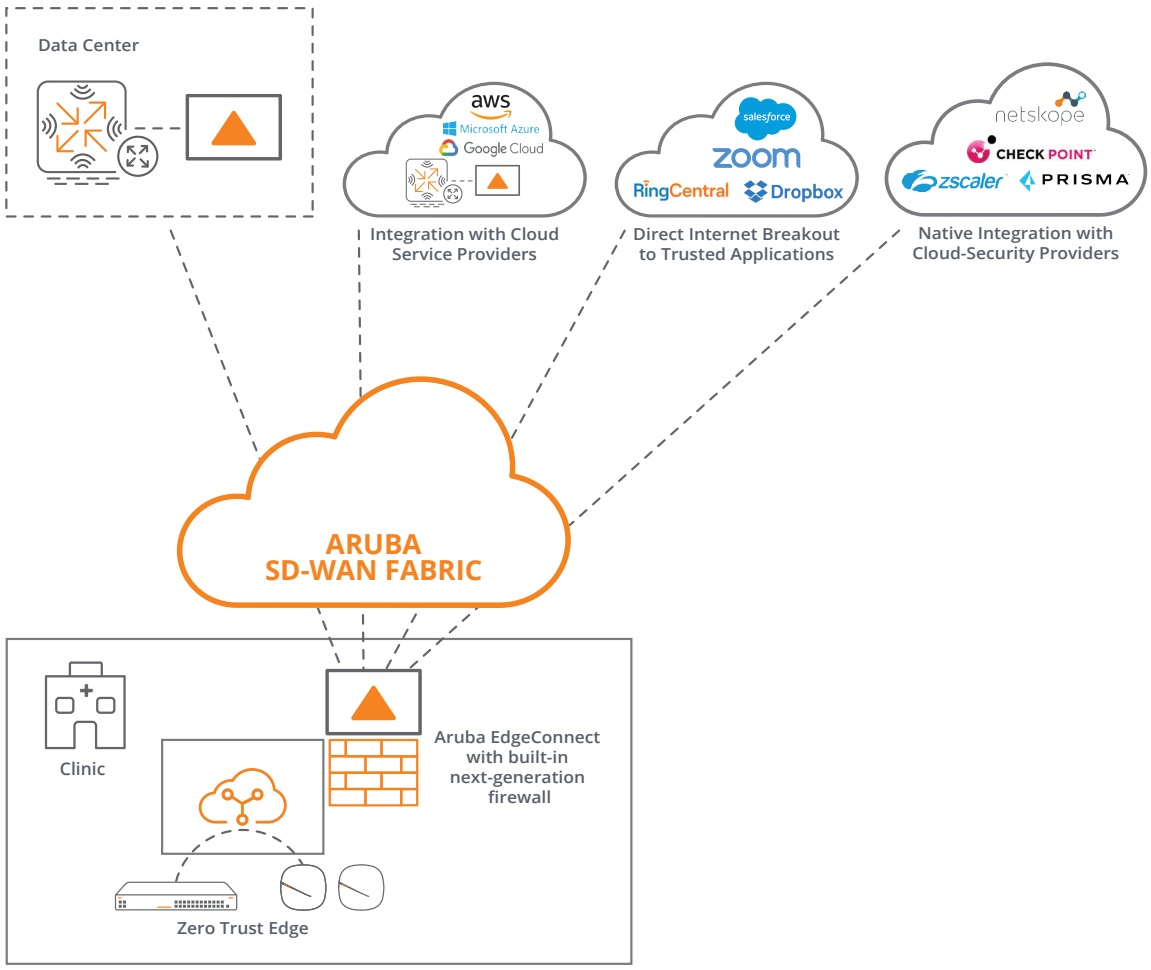
End-to-end connectivity to cloud providers: Aruba EdgeConnect Enterprise provides end-to-end connectivity to the cloud by deploying a virtual instance of EdgeConnect in any or all the four major public cloud providers. Healthcare organizations can also easily move workloads from one cloud provider to another, for example from AWS to Azure.

Best-of-breed SASE: With its advanced SD-WAN features, Aruba EdgeConnect Enterprise is the foundation of a robust SASE architecture. It natively integrates with leading third-party security capabilities such as CASB (Cloud Access Security Broker), SWG (Secure Web Gateway), and ZTNA (Zero Trust Network Access), enabling healthcare providers to implement advanced internet threat protection based on best-of-breed vendors.



A secure SD-WAN combined with cloud-hosted security service delivers a best-of-breed SASE architecture

Thanks to the First-packet iQ application classification feature, Aruba EdgeConnect Enterprise automates the orchestration to these solutions while traffic from suspicious applications is sent to the data center for further inspection. The integration with cloud security vendors is fully automated enabling healthcare providers to deploy security partner services in minutes.



Aruba EdgeConnect Enterprise enables a SASE architecture by automating orchestration to cloud security vendors

Use Case #3: Deliver the best telemedicine experience

Telemedicine relies on multiple applications that can be used to support different services, including wireless tools, email, two-way video conferencing, smartphones, and other telecommunications technology methods.

Telemedicine is driven by four concepts, each requiring different applications or supporting technologies for the communication or exchange of data:

- **Real-time telemedicine** comprises real-time contact between patients and healthcare practitioners via the use of a variety of applications that vary from a simple telephone conversation or email to a complex robotic surgery involving real-time consultation with remotely located specialists.
- **Store and forward systems** involve technologies like PACS (picture archiving and communication system), the medical imaging technology used primarily by healthcare organizations to securely store and digitally transmit electronic images and clinically relevant reports.
- **Home health-based telemedicine** involves remote patient monitoring (e.g., patient statistics and vital sign monitoring) from a distant location using a typical landline, wireless or internet connection as the communication transport service between the patient and the care center.
- **Mobile telemedicine** takes these applications out into the field, perhaps in the form of a mobile EMT vehicles or even a ruggedized backpack. It is used by first responders to communicate patient conditions and vital statistics in real-time with doctors located back at a hospital or other urgent care facility.

As healthcare becomes more data-driven and relies more on distributed care enabled by telemedicine, a high performance, low latency WAN is imperative. Reliable, high-quality communication is critical to the successful deployment of telemedicine programs.

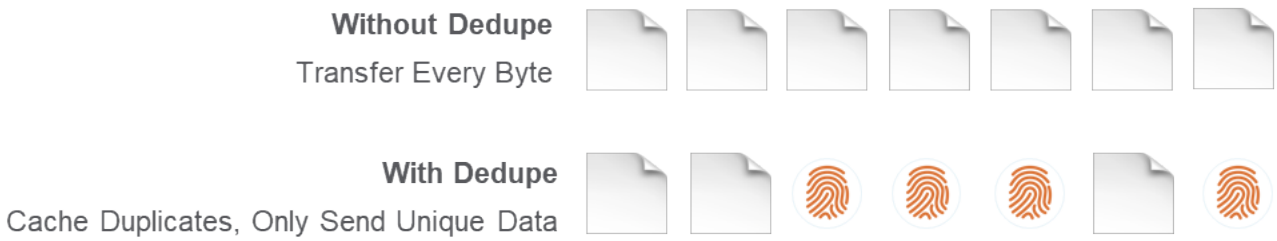
Telemedicine services are challenging to deploy using traditional WAN architectures:

- Real-time or interactive healthcare requires high quality video, teleconferencing, phone calls, online communications, and other technologies. Highly reliable and resilient wide area network connectivity is of paramount importance.
- Store-and-forward virtual medicine involves storage and fast transmission of vast amounts of medical information across the network. Traditional WAN architectures might support fast transmission of large files across the network with MPLS, but it comes with a prohibitive cost and dependency on slow delivery times.
- Home-based healthcare including remote patient monitoring and other tools like imaging and visualization, collaboration and sharing, require a secure, high performing and reliable network connection to transfer patient data in a timely manner and for vital problems such as heart problems or diabetes.
- Mobile telemedicine, used by first responders, requires reliable and resilient connectivity to ensure the real-time transfer of critical patient information. The main challenge here is to achieve uninterrupted connectivity across common cellular signals required for remote, mobile emergency telemedicine services.

Aruba EdgeConnect Enterprise SD-WAN delivers the robust wide area network required to offer high quality telemedicine services. Telemedicine applications require high-performance network connectivity with low latency in addition to highly reliable connections to ensure high-quality patient to healthcare provider communications.

Aruba EdgeConnect Enterprise overcomes the challenges of traditional WAN infrastructure by:

- **Prioritizing life-critical applications.** Providing reliable connections for medical experts performing operations remotely, or in case of an emergency, is critical. SD-WANs can utilize any underlying transport including MPLS, broadband internet, and LTE. It improves reliability through network redundancy or automated failover in case of network outage. It routes critical applications on the fastest paths and provides uninterrupted connectivity across common cellular signals required for mobile emergency telemedicine services.
- **Improving real-time application performance and reliability** by utilizing features such as tunnel bonding for real-time traffic steering across any combination of WAN transports and path conditioning to overcome the adverse effects of dropped and out-of-order packets common with internet connections. This highly reliable WAN architecture provides continuous availability of healthcare services and delivers the highest patient-staff quality of experience for real-time voice and video communications.
- **Accelerating the transfer of patient data** to overcome the effects of latency by applying TCP protocol acceleration as well as data deduplication and compression with Aruba WAN Boost. TCP Acceleration overcomes delays caused by window scaling and acknowledgment procedures in latent environments. Deduplication removes duplicate data and replaces it with a fingerprint and a pointer so that only the necessary data is transmitted across the WAN. Data compression leverages an LZ (Lempel-Ziv) compression algorithm to reduce the amount of data transmitted.
- **Securing the transfer of sensitive patient health records** and helping organizations achieve and maintain HIPAA compliance by combining the power of a next-generation firewall and network micro-segmentation. The EdgeConnect platform automates the configuration of cloud-hosted security services like Zscaler and Netskope to maintain network security policy compliance without compromise.



Data reduction: Eliminate overhead of redundant packets traversing the WAN with Aruba WAN Boost

Use Case #4: Improve security of Electronic Medical Records and IoT devices with a zero-trust network

Electronic Medical Records (EMR) are stored on-premises or in-the cloud. They can be accessed and updated from anywhere, but this poses increasing cybersecurity challenges. The number of data breaches involving patient records have indeed exploded in the last recent years to over 44 million records in 2021[10]. Additionally, these systems lack interoperability between competitive systems so that medical records are duplicated in several locations increasing the risks of being victim of a data breach.

IoT has transformed healthcare by offering new ways of treating patients and monitoring health. Their scope of use continues to grow exponentially with applications ranging from cancer treatments, wearables to sensors and medical alerts. The security of these devices has therefore become critical to provide the best treatment and ensure that they don't threaten patient health.

In the past few years, the number of IoT devices has skyrocketed increasing the attack surface and exposing healthcare providers to more cybersecurity risks. IoT devices are indeed difficult to secure as they cannot run security agents and often lack authentication systems, and they also become more vulnerable as they age. However, replacing legacy devices is often technically and economically unviable, not to mention highly disruptive to on-going operations.

To overcome these challenges, Aruba EdgeConnect Enterprise has earned the Secure SD-WAN certification from ICSA Labs thanks to its advanced SD-WAN and security features.

ICSA Labs Secure SD-WAN certification requirements include:

- **Advanced SD-WAN features** such as tunnel bonding, dynamic path selection and zero-touch provisioning
- **Native support (or via service chaining) for advanced security** functions such as next-generation firewall, anti-malware, intrusion prevention and DoS protection
- **Encryption** of sensitive data, as well as administrative and operational communications
- **Policy enforcements** for both WAN-specific functions and security policies
- **Security events logging**

Beside integrating advanced SD-WAN capabilities, Aruba EdgeConnect Enterprise embeds an application-aware next-generation firewall, with zero-trust segmentation, and identity-based access control capabilities, as well as IDS/IPS and DDoS defense to protect hospitals from malicious activities.

Zero-trust segmentation separates the traffic of life-critical applications from the rest of the traffic such as HVAC systems or surveillance cameras. It prevents an attack from spreading across the network and hitting critical applications such as EMR systems. Additionally, Aruba EdgeConnect Enterprise paired with Aruba ClearPass Policy Manager, implements a zero-trust policy approach assuming that no user or device is trusted by default, using identity and role-based access control.

Aruba ClearPass Policy Manager indeed adds identity knowledge of users, devices and roles with authentication capabilities such as RADIUS, TACACS+, and OAuth2 to manage network access and enable a dynamic segmentation, anywhere on the network – wired or wireless infrastructure. Through role-based access policies, IoT devices are automatically assigned the proper access control policy and dynamically segmented from other users and devices.

Aruba EdgeConnect Enterprise is able to apply security policies across the entire SD-WAN fabric rather than manually applying many individual policies for each location, creating one single logical firewall. An independent security policy can be applied for each segment, defining the security policies to enforce for the device traffic. Security policy changes are configured centrally and automatically distributed to hundreds or thousands of locations in minutes.

Additionally, the built-in firewall includes intrusion detection and prevention capabilities (IDS/IPS) to monitor, flag and drop traffic in case of a security threat. Threat events can be streamed to Security Information and Event Management (SIEM) systems for log review. Aruba EdgeConnect Enterprise also detects and prevents DDoS attacks such as protocol attacks, ICMP floods, and SYN floods. Using firewall protection profiles, the solution limits the number of malicious requests with actions such as rapid aging, drop excess, and block source.

[10] Source: July 2021 Healthcare data breach report, Hipaajournal.com, July 2021

	Patient monitoring devices	Unsecure IoT	Electronic Medical Records	Mission critical applications	HVAC	Inventory tracking for medical supplies	Business applications
Patient monitoring devices	✓	✓	✗	✗	✗	✗	✗
Unsecure IoT	✓	✓	✗	✗	✗	✗	✗
Electronic Medical Records	✗	✗	✓	✓	✗	✗	✗
Mission critical applications	✗	✗	✓	✓	✗	✗	✗
HVAC	✗	✗	✗	✗	✓	✓	✗
Inventory tracking for medical supplies	✗	✗	✗	✗	✓	✓	✗
Business applications	✗	✗	✗	✗	✗	✗	✓

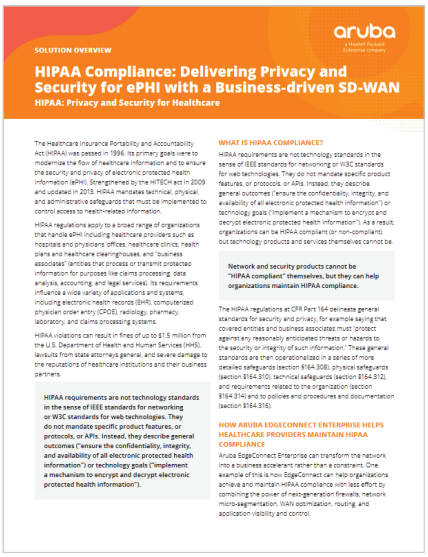
Zero-trust segmentation isolates and segments network traffic based on role-based security policies

Use Case #5: HIPAA compliance: Delivering privacy and security for ePHI with a business-driven SD-WAN

The Healthcare Insurance Portability and Accountability Act (HIPAA) was passed in 1996. Its primary goals were to modernize the flow of healthcare information and to ensure the security and privacy of electronic protected health information (ePHI). Strengthened by the HITECH act in 2009 and updated in 2013, HIPAA mandates technical, physical, and administrative safeguards that must be implemented to control access to health-related information.

Aruba EdgeConnect Enterprise secure SD-WAN helps healthcare organizations achieve and maintain HIPAA compliance by combining the power of a next-generation firewall, network micro-segmentation, WAN optimization, routing, and application visibility and control.

To learn more about how Aruba EdgeConnect Enterprise answers CFR Part 164 of HIPAA regulations, that delineates general standards for security and privacy, download our solution overview about HIPAA Compliance: Delivering Privacy and Security for ePHI with a Business-driven SD-WAN


SOLUTION OVERVIEW

HIPAA Compliance: Delivering Privacy and Security for ePHI with a Business-driven SD-WAN

HIPAA: Privacy and Security for Healthcare

HIPAA Compliance with Aruba EdgeConnect Enterprise

CONCLUSION

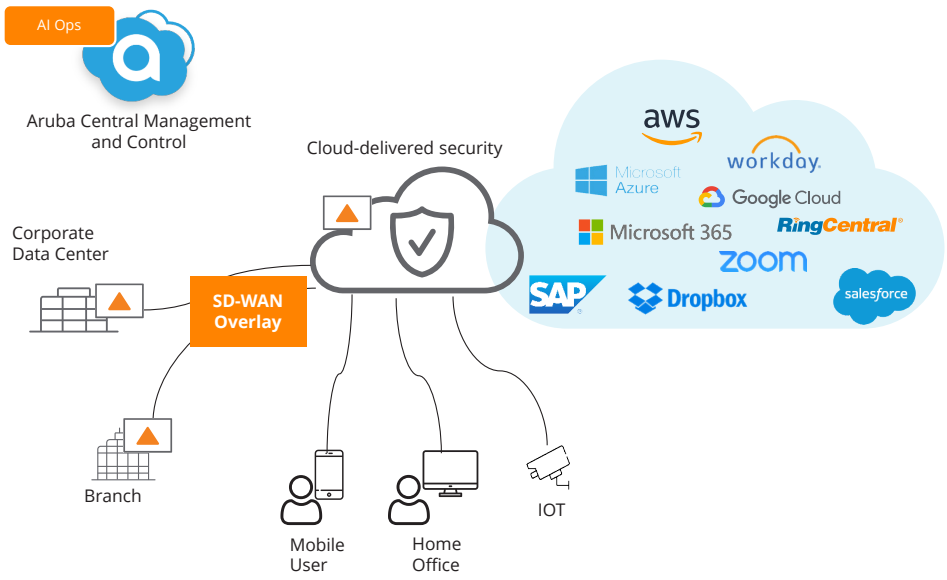
The COVID-19 crisis has profoundly impacted the healthcare sector and highlighted the need for greater access equity to care. Patients and medical staff now ask for more convenience and more personalized care. In that context, the healthcare sector is witnessing the rise of telehealth that has become the main vector of interaction for areas such as primary care and testing results. In addition, the healthcare sector is modernizing its facilities into smart hospitals using a myriad of IoT and imaging devices as well as medical records now stored electronically. This has resulted in an increased attack surface exposing healthcare providers to significant data breaches and cybersecurity issues.

To tackle these challenges, healthcare providers need to:

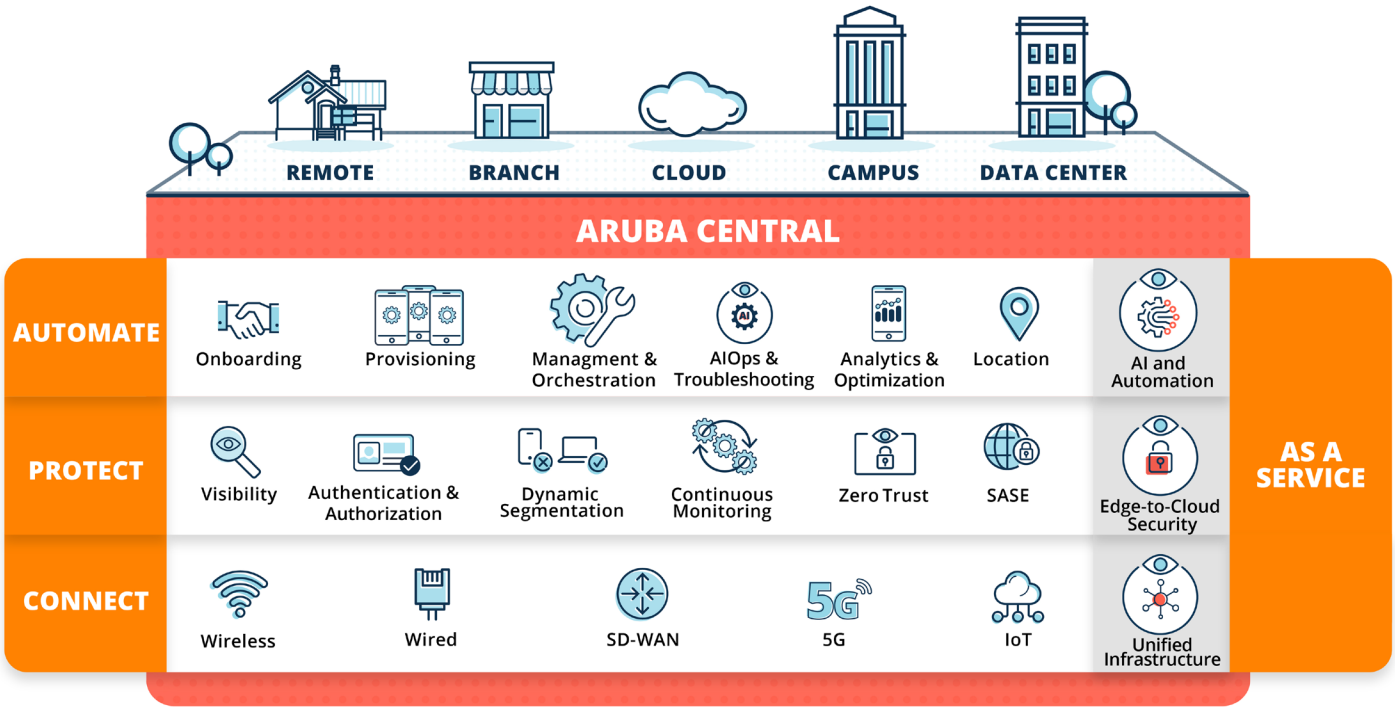
- Implement reliable network connectivity especially for life-critical applications
- Support cloud-first, geographically distributed organizations
- Accelerate the use of telehealth
- Secure electronic health records (EHR) and IoT devices
- Ensure HIPAA compliance

In summary, Aruba EdgeConnect Enterprise SD-WAN platform helps healthcare providers address the five key challenges:

1. Implement reliable network connectivity by virtualizing network connections, enabling healthcare providers to bond heterogeneous links, including broadband internet, MPLS and 5G/LTE connections to ensure network redundancy for reliability and highest Quality of Service.
2. Support cloud-first geographically distributed organizations with seamless integration with the five largest global public cloud providers – AWS, Google Cloud, Oracle, Microsoft Azure, Alibaba Cloud as well as Microsoft 365 – increasing security and application performance. It provides the foundation for a robust SASE architecture by natively integrating with best-of-breed third-party cloud security capabilities.
3. Accelerate the use of telehealth with enhanced visibility through a single pane of glass and greatly simplifies the network infrastructure in remote locations by incorporating many features such as a router, a firewall and WAN optimization capabilities. Constant monitoring of network conditions and quickly adapt to route the traffic to the best path.
4. Securing electronic health records is ensured with built-in next-generation firewall and Aruba ClearPass Policy Manager, that enforces a zero-trust policy approach through micro-segmentation. The firewall indeed creates a logical separation between life-critical applications, electronic medical records, IoT devices, and non-critical traffic, limiting the spread of cyberattacks and malware.
5. Ensure HIPAA compliance through end-to-end network segmentation, the enforcement of strong encryption of data in motion, and a tight integration with cloud-security vendors.



Aruba EdgeConnect Enterprise is the foundation of a robust SASE architecture that enables healthcare providers to choose from the best-of-breed security capabilities



The three layers of Aruba Edge Services Platform.

Aruba EdgeConnect Enterprise is a key component of the Aruba Edge Services Platform (ESP) that enables a unified approach to centrally manage all security and network aspects including wireless, LAN and WAN connectivity with common zero trust and SASE security frameworks spanning the entire portfolio. Aruba advanced AIOps capabilities automatically and continuously monitor network, and application performance as well as security policy enforcement, enabling automated remediation to impairments or potential threats.

BP_SD-WANforHealthcare_SK_100322 a00126775enw

Contact us at www.arubanetworks.com/contact