

Improving patient care, while adhering to HIPAA regulations

Case Study



Christus Health is a Catholic, not-for-profit system made up of more than 600 centers, with over 15,000 physicians across community hospitals and walk-in clinics. It engaged Netskope to help modernize multiple facets of Christus Health's networking infrastructure, particularly during the pandemic, where distributed healthcare became a requirement. Legacy firewall-based site-to-site and remote access VPN systems provided solid remote access connectivity in their day, but more powerful and nimble technologies have now rendered them obsolete, resulting in high operational costs for this \$6B healthcare system.

The Challenge

Healthcare organizations are under increasing pressure to reduce IT staff and cut CAPEX and OPEX costs. They have to adapt quickly to changing times and offer secure, reliable distributed healthcare. These forces are driving demand for automation and the need for technologies with high operational efficiency.

Key Challenges:

- **High CAPEX cost for legacy hardware-based firewalls**
- **Increasing OPEX cost to deploy and maintain firewall-based VPNs**
- **Ongoing connectivity and link quality issues for remote teleworkers**
- **Security concerns for staff in school-based clinics**
- **Need to offer secure, reliable distributed healthcare**

Traditional site-to-site VPNs require expensive firewall hardware devices to be deployed at every site. The typical CAPEX cost per site can be high, plus there is an additional OPEX for annual maintenance contracts. To make matters worse, extensive manual configurations are required throughout the deployment process. Average deployment times per site often exceed two days and hinder valuable IT networking staff from focusing on more strategic operations.

The Solution

Christus Health initially started by exploring first-generation SD-WAN solutions, but quickly found that CAPEX hardware costs and OPEX pricing and operational models failed to effectively address micro-branch and remote teleworker scenarios. Netskope enabled Christus Health to achieve high-quality connectivity and streamlined operational efficiency at a fraction of the cost.



Profile

Industry Healthcare	Region Southern US	Employees 30,000
-------------------------------	------------------------------	----------------------------



[Click here to visit the Christus Health website](#)

Challenges

- Excessive operational costs associated with legacy hardware, including firewall-based VPN
- Inconsistent experience with application performance for remote workers
- Security concerns for school-based clinics
- Need to rapidly migrate to telehealth

Results

- Zero trust-based security for clinics inside public schools
- Over 10x TCO savings
- Met secure telehealth need from COVID-19
- Micro-segmentation for medical IoT

Benefits at a Glance

- Netskope Borderless SD-WAN solution delivers 10x TCO savings
- Cutting-edge automation enables one-click edge activation
- Critical application traffic is automatically prioritized
- Zero Trust security is provided by granular control of traffic flows and isolated trust boundaries, as well as built-in stateful firewalling

School-based Clinics

Christus Health was able to extend secure connectivity with zero trust principles to medical staff who work out of school-based clinics. Netskope Borderless SD-WAN enabled medical staff to securely access enterprise hospital data center resources from within the much less secure public-school systems' networks. This is a timely solution given the fact that many school networks, including the state of Louisiana, have faced an ongoing security crisis with ransomware attacks.

Business Benefits

Netskope Borderless SD-WAN has unlocked many use cases which would have been unthinkable with past technologies. Netskope has a highly efficient code base, which runs on cloud-native technologies delivering solutions that deliver over 10x in TCO savings. Christus Health is leveraging Netskope for a variety of use cases from secure telehealth to medical IoT.

Secure Telehealth - COVID-19

Essential staff such as IT operations rely on Netskope to deliver a high-quality, reliable remote telehealth solution. Netskope Borderless SD-WAN is ideal for extending low-cost secure wired or wireless WAN access to essential business staff members who require optimized connectivity as they ensure that critical patient care systems are online and available to all hospitals and clinics.

Looking Ahead

Many critical medical systems that transmit sensitive patient information are based on outdated or insecure protocols. The organization's IT department is currently looking to expand the deployment by using it to secure legacy medical systems within the private enterprise network. Netskope Borderless SD-WAN can be used to secure communications from a medical IoT device such as a CT machine to back-end imaging servers in the data center. This type of solution could represent a significant cost savings when compared with similar solutions that involve the deployment of legacy systems.

“As we continue to transform our patient care experience, we are excited to partner with Netskope. Netskope Borderless SD-WAN provides adaptive, identity-aware precision access for our medical workers to deliver care from the comfort of their homes, without compromising experience, all at a significantly lower cost to our business. In the future we see many applications for Netskope, including our medical IoT deployments.”

– Rick Lacy, Sr. Enterprise Network Engineer, Christus Health



Netskope, a global cybersecurity leader, is redefining cloud, data, and network security to help organizations apply Zero Trust principles to protect data. The Netskope Intelligent Security Service Edge (SSE) platform is fast, easy to use, and secures people, devices, and data anywhere they go. Learn how Netskope helps customers be ready for anything on their SASE journey, visit [netskope.com](https://www.netskope.com).