Zero Trust security with high-performance connectivity

Case Study

In 1892, Andrew Taylor Still founded A.T. Still University (ATSU), the nation's first institution of osteopathic healthcare. Since then, it's been a leading health sciences university, comprised of two campuses (in Kirksville, Missouri, and Mesa, Arizona) on more than 200 acres housing six prestigious schools. ATSU has dental clinics in Arizona and Missouri, and partners with 12 community health centers across the nation. Its culturally rich learning environments include residential and online healthcare-related graduate degrees, along with community-based partnerships worldwide. ATSU has more than 1,300 employees dedicated to its not-for-profit mission, and an average annual enrollment of over 3,100 students from 35 countries.

The Challenge

ATSU was using a software-based VPN client for its remote workers to provide connectivity to an application hosted in its data centers over an internet WAN link. The VPN connection from remote workers was terminated at a VPN server (cluster) deployed at the data center. The ATSU IT team was also managing large university sites with legacy routers using an expensive MPLS circuit and backup internet. The lean IT team was forced to manage two different legacy solutions that involved considerable complexity and operational overhead.

ATSU's remote education staff and students suffered performance issues with voice and real-time video applications over lossy internet links. Exacerbating the problem, there was no option to prioritize critical applications over bandwidth-consuming streaming applications (e.g., Netflix, YouTube). As a result, end-user experience was poor, with frequent VPN client disconnects to the primary data center, as well as increased latency due to single-homed connectivity adding to the problem.

The ATSU IT team had a high total cost of ownership (TCO) fueled by expensive infrastructure and operational complexity. University students using Guest Wi-Fi and high-priority-demanding voice and video applications put pressure on the available MPLS bandwidth. Upgrading the MPLS circuit would increase the university costs significantly. Moreover, installing, configuring, operating, and managing two different network islands for remote workers and university sites was complex, time-consuming, and expensive.

ATSU started exploring alternative options to have a unified network policy for remote workers and university sites while improving application performance without compromising security. It required a solution that could deploy quickly, provide security, enable better visibility, limit downtime, and deliver exceptional user experience. Additionally, the university's sites require high availability with simplified routing.

ATSU | A.T. Still University
FIRST IN WHOLE PERSON HEALTHCARE

Profile

Industry
Education and Healthcare

Region
United States

Click here to visit the ATSU website

Challenges

- Complicated, disparate network islands
- Inconsistent application performance for remote workers
- Traditional MPLS design with limited bandwidth at universities

Results

- Achieved PCI and HIPAA compliance with ease
- Ease of deployment with unified cloud-native policy
- Automatic, secure connectivity at scale
- Assured application performance
- Simplified day-2 operations
- Lowered TCO by 10x

Compliance and Zero Trust Security With Netskope Borderless SD-WAN

ATSU began deploying Netskope Borderless SD-WAN for remote workers by deploying the Netskope SASE Gateway at each location and connecting it to the cloud-delivered Netskope SASE Controller. Using the internet as transport, all remote staff could easily and securely connect to applications hosted in the data center. This provided enterprise-level connectivity with intelligent path selection and link remediation. With the success of remote staff deployment, ATSU expanded the Netskope solution deployment for its university sites.

Ease of Deployment With Unified Cloud-native Policy

Netskope Borderless SD-WAN was deployed with one-click activation using a unified cloud policy, that the remote staff could activate themselves from their homes. Netskope enabled easy integration with ATSU data center's core routers.

Automatic, Secure Connection

With the Netskope SASE Gateway's Network Security feature, a secure overlay is automatically created between the edges. ATSU remote staff could connect to redundant data centers with a secure overlay for high availability using a one-click centralized policy without requiring complex configuration.

Additionally, Netskope provided secure access by deploying zero trust principles to control traffic flows and isolate trust boundaries, enabling identity-aware-per-app access policies for the end-user, as well as through application-aware stateful firewall and filtering of unwanted content categories.

Assured Application Performance

Netskope at the edge (including wireless) greatly improved voice and video collaboration experience. Business-critical applications are now automatically prioritized with sufficient bandwidth allocation, with assured application performance. Netskope built-in remediation ensures performance protection against link degradation on all paths.

Simplified Day-2 Operations

Netskope SASE Orchestrator provides a single pane of glass for configuration, monitoring, and troubleshooting with deep visibility into network and edge health. The ATSU IT team was able to gain deep visibility into WAN metrics, devices connected to the edge, and enhanced application usage with flow-level details. With these insights, they could troubleshoot and resolve issues quickly. The IT team was able to perform a software upgrade without any downtime, avoiding after-hours schedule.

TCO 8-10x Lower Than Alternatives

Traditional wide area network (WAN) and infrastructure at geographically dispersed sites is expensive, with per-location costs reaching tens of thousands of dollars. ATSU was able to purchase inexpensive circuits from carriers, and use Netskope Borderless SD-WAN architecture to deliver high-quality video, voice, and data to each facility in the network.

> "Netskope allows ATSU to enable remote working and learning overnight for our schools, clinics, and remote workers, while helping us meet HIPAA compliance. Netskope Borderless SD-WAN helps us meet our objectives for zero trust and is ideal for our remote deployments, ultimately resulting in more affordable tuition and better healthcare services."
>
> – Garrett Holthaus, Network Engineer, ATSU

netskope

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.