



# A.T Still University Achieves Compliance, Zero Trust Security and IT Agility with InfioT

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, MO; and Mesa, AZ) 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.

## HEADQUARTERS

KIRKSVILLE, MO

## INDUSTRY

EDUCATION and HEALTHCARE

## CHALLENGES

- Complicated, inconsistent 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

## The Challenge

ATSU was using a software-based VPN client for their remote workers to provide connectivity to the application hosted in 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 expensive an MPLS circuit and backup Internet. The lean IT team was forced to manage two different legacy solutions that involved lots of complexity and operational overhead.

ATSU’s remote education staff and students had performance issues with voice and real-time video applications over lossy Internet links. Furthermore, there was no option to prioritize critical applications over bandwidth-consuming streaming applications (e.g. Netflix, YouTube). So, end-user experience was poor, owing to frequent VPN client disconnects to the primary data center, as well as increased latency due to single-homed connectivity.

The ATSU IT team had a high total cost of ownership (TCO) due to its expensive infrastructure and operational complexity. University students using Guest WiFi and high-priority-demanding voice and video applications caused pressure on the MPLS bandwidth. Upgrading the MPLS circuit would increase the cost 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 be deployed quickly, and that was secure, provided better visibility, limited downtime, and delivered exceptional user experience. Additionally, university sites required high availability with simplified routing.

“ *Infiot AI Powered Intelligent Access allowed ATSU to enable remote working and learning overnight for our schools, clinics, and remote workers, while helping us meet HIPAA compliance. Infiot's thin wireless edge with zero trust security is ideal for our remote deployments, ultimately resulting in more affordable tuition and better healthcare services.* ”

*Garrett Holthaus,  
Network Engineer  
ATSU*



## Compliance and Zero Trust Security with Infiot

ATSU began deploying the Infiot solution for remote workers by deploying the Infiot thin, wireless edge at each location and connecting it to the cloud-delivered Infiot Management and control plane. Using 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 Infiot solution deployment for their university sites.

## Ease of Deployment With Unified Cloud-Native Policy

Infiot thin, wireless edges were deployed with one-click activation using a unified cloud policy, that the remote staff could activate themselves from their homes. Infiot enabled easy integration with ATSU data center's core routers.

## Automatic, Secure Connection

With Infiot Cloud-Scale VPN, a secure overlay is automatically created between the edges. ATSU remote staff could connect to redundant data centers with secure overlay for high availability using a one-click centralized policy, without requiring complex configuration.

Additionally, Infiot 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

Infiot thin, wireless edges greatly improved voice and video collaboration experience. Business-critical applications are automatically prioritized with sufficient bandwidth allocation, thereby assuring application performance. Infiot built-in remediation ensures performance protection against link degradation on all paths.

## Simplified Day-2 Operations

Infiot Management 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 Infiot Intelligent Access architecture to deliver high-quality video, voice, and data to each facility in the network.