



CASE STUDY

SECURE ACCESS ACROSS HYBRID ENVIRONMENTS

Austin Lighthouse Uses SDP to Secure Access Across Hybrid Environments and Adopt Zero Trust

BACKGROUND

Austin Lighthouse, Travis Association for the Blind, founded in 1934, is a service-oriented 501(c)(3) non-profit organization that offers education, training, advocacy and community for blind and visually-impaired individuals in Travis County and surrounding areas.

Its mission is to assist people in building or restoring their independence through skills training, education and employment opportunities that encourages them to be gainfully employed, become involved in their local community, and give voice to blind and visually-impaired Texans.

THE CHALLENGE

Austin Lighthouse was concerned with potential security vulnerabilities of its existing VPN solution and wanted to adopt a Zero Trust approach to security. The organization was looking for a more secure access solution to address both remote users and on-prem employees and to enable secure access across hybrid environments including its Azure environment. Additionally, Austin Lighthouse needed to jumpstart its CMMC compliance journey.

THE SOLUTION

Working together with partner Clarify360, Austin Lighthouse evaluated different options to address its security needs. Ultimately Austin Lighthouse selected Appgate’s Software-Defined Perimeter (SDP) platform that supported both remote and on-premises users with a unified policy approach. Appgate SDP is a Zero Trust Network Access (ZTNA) solution that applies the principles of Zero Trust to deliver fine-grained access control. It provides dynamic, user-centric access control, creating an individual network segment of one, based on simple policies.

The platform is context-aware to ensure that users can only access those network resources and applications to which they’re specifically entitled—via secure mutually encrypted tunnels to prevent lateral movement to unauthorized network resources. The net effect is that everything else on the network is invisible and unreachable. This results in a Zero Trust network architecture, enforcing least privileged access when compared to the broad access of Austin Lighthouse’s previous VPN solution.

The result for Austin Lighthouse employees was seamless access – via a consistent user experience regardless of user location whether on-prem or working remotely.

The customer also mentioned that by deploying Appgate SDP, they have jumpstarted their journey to CMMC compliance.

INDUSTRY

501(c)(3) Non-profit

CHALLENGES

VPN replacement for remote users

Secure access for on-prem employees

Adopt Zero Trust

Jumpstart their CMMC compliance journey

SOLUTION

Appgate SDP

BENEFITS

Improved network access security

Fine-grained access control

Improved user experience

Simultaneous encrypted connections to multiple sites

Protects hybrid access into Azure environment



“When it comes to network security there is no such thing as too little information or too much security. Zero-trust networks trust no one!

Irrespective of whether a user has accessed those same resources before or not. Any user or managed device that attempts to access resources within a zero-trust network must go through strict verification and authentication processes, even if that person or client is on premises in our office. After researching various options, we chose Appgate. Appgate’s offering allowed us to make an immediate and material impact towards our cybersecurity needs.”

-Alonso Perales, Vice President – Business Innovation, Austin Lighthouse