CASE STUDY

8 Location Heavy Equipment Company

PRIMARY & SECONDARY INTERNET, SD-WAN, MANAGED SECURITY



Challenges

Aging Network Infrastructure: Outdated networking equipment created the need for a comprehensive technology refresh to improve performance, security, and long-term scalability.

Limited Visibility & Control: The customer needed greater insight into circuit performance, device management, and network activity, along with the flexibility to make changes without relying entirely on their provider.

Business Continuity: Dependence on reliable connectivity for daily operations and cloud-based applications created a need for redundant internet connections and improved network resiliency.

Complex Cloud Connectivity & Security: Securely connecting multiple locations to centralized firewall infrastructure and a managed cloud provider required a more streamlined, consistent approach to traffic routing and security.

Telesystem
IT's About Trust

About the Customer

A leading bulk and heavy equipment hauling company specializing in trailer sales, service, and repairs needed to modernize its aging network infrastructure across **eight locations in five states.** Serving the construction, agriculture, transportation, and bulk hauling industries, the organization relied on secure, dependable connectivity to keep its geographically dispersed operations running efficiently.

As the business evolved, its existing technology environment required a refresh. Managing network infrastructure across multiple locations created challenges with visibility, control, and consistency. The company needed to consolidate its network, strengthen security, and establish a more reliable foundation for cloud-based applications and daily business operations.

The organization turned to Telesystem to design and deploy a comprehensive, fully integrated networking solution.

Telesystem's Solution

Telesystem implemented **primary and secondary internet connections** at all eight locations, providing redundant connectivity to minimize disruptions and maintain business continuity. **Fortinet FortiGate SD-WAN**, along with **Fortinet PoE switches and wireless access points,** created a standardized network environment designed to improve performance, simplify management, and strengthen security across every site.

To further enhance protection, Telesystem established secure **IPsec VPN tunnels** connecting each location to a centralized Telesystem cloud firewall. Network traffic is routed through this centralized security environment, while Desktop-as-a-Service (DaaS) traffic travels securely through IPsec tunnels to the company's managed cloud provider.

The customer also gained greater visibility and control through **Telesystem's co-managed FortiGate solution** and **circuit monitoring portal,** enabling its IT team to monitor network performance, manage devices, and troubleshoot issues more efficiently while maintaining access to Telesystem's 24/7 U.S.-based support.

The result is a **modernized, secure, and resilient network** spanning Florida, Georgia, North Carolina, South Carolina, and Texas. By consolidating connectivity, security, and network management with Telesystem, the organization gained greater visibility, stronger protection, and improved resiliency across all eight locations. With centralized security, redundant connectivity, and a flexible co-managed approach, their IT team can maintain control of its infrastructure while relying on Telesystem's 24/7 U.S.-based support to keep operations connected and moving forward.