Zscaler Blog

Get the latest Zscaler blog updates in your inbox

Subscribe

EXPERT INSIGHTS | CUSTOMER SUCCESS STORY

Copy URL

Founded in 1980 and proudly family owned, Maverick Transportation built our reputation on safety, technology, and innovation. We specialize in exceptional flatbed, glass, and marine transportation services, serving customers across the central and eastern United States with a fleet of over 1,500 trucks and a dedicated team of over 2,000 employees.

Our people are the backbone of our business—from professional drivers on the road to headquarters team in Little Rock, Arkansas, to securement specialists and semi-truck technicians at shipping offices and contracted customer sites. We rely on Zscaler to provide our teams with access to the internet, SaaS, and private apps they need while protecting our business from ever-present and evolving cyberthreats. Our multi-year Zscaler journey has optimized the distributed work experience for our users, protected our business, and simplified IT operations.

Now we're taking the next step with Zscaler Cellular.

Empowering our workforce with seamless, secure access

We began our zero trust journey in 2021 to empower secure work-from-anywhere for our employees. Before Zscaler, most of our corporate staff relied on thin clients and virtual desktop infrastructure (VDI), while about 20% had Windows laptops and used a remote access VPN client when off site. As our distributed workforce relied more heavily on voice and video to collaborate, the VDI user experience degraded. With our business dependent on more demanding applications, we wanted to modernize our endpoint strategy, retire our VDI and VPN, and adopt zero trust networking best practices.

With Zscaler Private Access (ZPA), our corporate staff have fast, secure, and reliable access to our private apps from anywhere. The user experience dramatically improved and we retired our VDI environment and VPN clients for laptops. The zero trust network access (ZTNA) model significantly reduced our attack surface and minimized the risk of lateral movement within our network.

Zscaler Digital Experience (ZDX) allows our IT team to proactively monitor and resolve performance issues across apps, networks, and devices—before they impact users. Zscaler Deception actively defends and fortifies our endpoints against advanced threats, with early detection of ransomware and credential abuse. Integrating our identity provider and endpoint protection solutions with Zscaler not only removes friction—it makes security smarter.

We also replaced our legacy web filtering solution with Zscaler Internet Access (ZIA) for cloud native, AI-powered protection for our web and SaaS apps. Employees enjoy fast, reliable, and safe access from their laptops or tablets to the apps and digital resources they need. With our Zscaler investments we were also able to consolidate down from multiple mobile device management (MDM) software platforms to manage company-provided and company-managed devices, which also means IT has fewer products to buy and manage.

Our zero trust journey with Zscaler lowered cyber risk, strengthened business continuity, and gives us a future-ready infrastructure that empowers our team to deliver excellence every mile of the way.

Zero trust security for cellular-connected IoT and mobile devices

We were introduced to the Zscaler Cellular Service at last year's Zenith Live, where we learned we could extend Zscaler's zero trust security model to cellular networks. This innovation immediately caught our attention because it solved a long-standing challenge: how to effectively secure IoT and mobile devices at our clients' and customers' properties we operate in where we have no control of the networking options provided or the operating environment without adding software agents or using remote access VPNs.

Zscaler ZPA had allowed us to retire our traditional VPN solution for our corporate laptops, but we still needed a VPN solution for certain locations with shared use mobile hardware where users couldn't connect using an otherwise secured corporate network. Our managed employees, for example, work on site at customer locations and use a shared tablet kiosk for logging hours and work. They need access to Maverick systems, but connecting to a customer's Wi-Fi meant additional network and cybersecurity policies.

The traditional VPN we used for these tablets was being provided by an MDM platform we were looking to replace for further consolidation, and the MDM products' VPN implementation was both problematic to ensure ongoing reliability for connectivity and was not for the zero-trust security operating model. We attempted to use ZPA for these shared devices, but because the access was enabled through identity-based authentication, employees had to conduct two-factor authentication every time they wanted to use the device and then log in again separately to the applications they were using.

In essence, we saw The Zscaler Cellular Service as an opportunity to create device-bound authentication through Zscaler. This became our test case, and after equipping kiosks with Zscaler Cellular, our zero trust policies are enforced through the Zscaler Cellular Edge. The lines are gone, the employee experience is better, our business is still protected, and we don't need a software agent or VPN on the device.

Because we had high expectations for Zscaler Cellular, we purposely chose to test its efficacy at locations with historically poor connectivity. After all, the majority of our customers operate out of plants or other industrial sites with environmental factors that degrade connectivity. It would *have* to work in these locations, otherwise we wouldn't have confidence in a broader rollout.

Zscaler Cellular selects from multiple nearby carriers, which is beneficial in these industrial areas with poor signal penetration. Zscaler Cellular keeps devices connected to the best available cellular service, addressing any concern around connectivity.

Looking ahead: Securing Maverick's fleet vehicles and employee devices

After a successful pilot, we have confidence that Zscaler Cellular can work across challenging connectivity environments. We are excited to explore future business cases for zero trust cellular at Maverick.

As a company committed to safety, integrity, and employee well-being, our fleet vehicles and trailers are equipped with in-cab telematics units, trailer and load sensors, and driver safety cameras. These IoT devices and sensors require always-on, secure cellular connectivity. We see the potential to use Zscaler Cellular to enforce our zero trust policies, protect against IoT attacks, and deliver a more resilient mobile connection. Resiliency is especially important for an organization like ours, as drivers need consistent and reliable connectivity while on the move.

Another potential use case for Zscaler Cellular is to deliver a better, more secure experience for our district service managers. These employees travel nationwide to conduct truck and trailer maintenance reviews and perform maintenance servicing tasks. In several markets, we handle last-mile deliveries, where drivers are provided with company-issued cell phones for both our company and our contracted customers. In these use cases, we could use Zscaler Cellular to assure that drivers have reliable cell connectivity and our zero trust security policies are enforced wherever they go.

We also see the potential to use Zscaler Cellular to make living on the road better for our drivers. It's a demanding job and drivers can be away from home for a week or more. Maverick drivers have the opportunity to be provided a subsidized cellular hotspot device and service plan to make it easier to stay connected with family and friends. Zscaler Cellular could mean enhanced security, faster service, and better network coverage for our drivers—they could stream videos, games, or video chat from the comfort of their sleeper cabs, all without compromising our high standard for security.

***

For Maverick, our Zscaler zero trust journey has enhanced our employees' digital experience as they access the internet, SaaS, and private apps, strengthened the security of mobile and IoT devices, and simplified IT operations. We're just getting started with Zscaler Cellular and we're excited to experiment and innovate.