Zscaler Cellular & AT&T FirstNet®

DATASHEET

Overview

For first responders, mission assurance is an imperative. In critical situations, our emergency personnel rely on real-time data, situational awareness, and seamless communication to deliver life saving care and public safety. However, relying on a single carrier or legacy VPNs creates single points of failure and expands the attack surface. Our first responders require more than just assured connectivity. End to end secure delivery of SaaS and privately hosted applications is required.

When lives are on the line, first responders can't afford dropped sessions, slow reconnects, or "best-effort" security; yet many agencies still depend on single-carrier coverage, legacy VPN concentrators, and edge routers that create brittle choke points in the field. During major incidents, congestion and damaged infrastructure can degrade access to CAD, situational awareness, PTT/ROIP, and video workflows precisely when demand spikes; meanwhile, internet-exposed gateways and always-on vehicle/IoT connectivity expand the attack surface and increase the blast radius of a compromise.

Mission assurance now requires assured service delivery—connectivity engineered for disruption and security engineered for least privilege so responders can reach only the applications they need, regardless of which cellular network is available.

Agencies should adopt a robust cellular connectivity and security architecture designed for emergency conditions—one that eliminates single points of failure, maintains secure access through network transitions and congestion, enforces consistent Zero Trust policy across all cellular paths, reduces inbound exposure of field infrastructure, and provides unified visibility for both operations and security teams

Why Now?

Public safety operations have become mobile-first and application-dependent—CAD/RMS, video, mapping, real-time intelligence, and LTE/5G PTT are now required in the field, not optional. That shift increases the impact of congestion, coverage transitions, and infrastructure damage during major incidents, when demand spikes and conditions are least predictable. At the same time, agencies are expanding connected vehicles, routers, and IoT footprints, creating more edge exposure and making legacy VPN gateways a high-value target and operational choke point. The result is a widening gap between modern mission needs and legacy connectivity/security models driving urgency for resilient cellular service delivery with consistent Zero Trust controls.

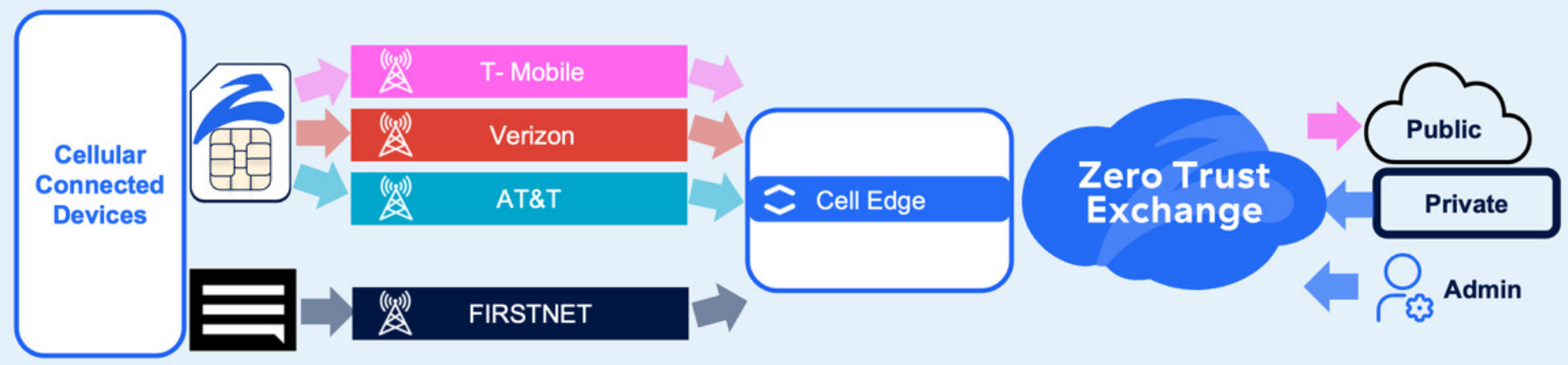
Given these pressures, agencies need an approach that combines priority connectivity during incidents with resilient failover and consistent Zero Trust security without adding operational complexity. This is exactly where a jointly engineered approach matters: one that pairs public-safety-grade network priority with a security and resilience layer built for disruption

Our Solution

What Zscaler brings to the table: secure cellular service delivery built for disruption

Zscaler Cellular extends the Zscaler Zero Trust Exchange to cellular-connected vehicles, routers, and IoT— so agencies can deliver mission-critical applications without relying on exposed VPN gateways or placing field assets on the internal network. It provides a consistent Zero Trust policy for cellular traffic, centralized enforcement and logging, and an architecture designed to maintain secure access through coverage transitions and degraded conditions. When deployed in dual-SIM routers, Zscaler Cellular also adds multi-carrier resilience so connectivity can automatically shift to the best available path while maintaining the same security posture and operational visibility.

The joint solution: Together, **AT&T FirstNet®** and **Zscaler Cellular** enable assured service delivery for public safety. FirstNet® provides priority and preemption for primary mission-critical connectivity, while Zscaler Cellular complements it with multi-carrier commercial fallback (in dual-SIM configurations) and end-to-end Zero Trust security enforcement. The result is secure, uninterrupted access to CAD, PTT/ROIP, video, and intelligence services for police vehicles, fire apparatus, and mobile command centers— without creating new choke points or security gaps when the network path changes.



Zscaler Cellular + AT&T FirstNet® redefines mission-critical service delivery. By combining the priority and preemption of FirstNet® with the multi-carrier resilience of Zscaler Cellular when used in dual-SIM applications, we deliver an unshakeable, Zero Trust foundation for public safety use cases. This solution ensures that police cruisers, fire apparatus, and mobile command centers maintain secure, uninterrupted access to critical dispatch, push-to-talk, and intelligence services under any condition. True end-to-end secure service delivery over any cellular network.

How It Works: The Zero Trust Advantage

Zscaler Cellular works by seamlessly uniting mobile networks (FirstNet® and commercial) with the Zscaler Zero Trust Exchange through the Zscaler Cellular Edge where internet security and microsegmented application tunnels are applied. This architecture removes the reliance on traditional "castle-and-moat" firewalls and VPN concentrators that create bottlenecks for cellular traffic. Unify the entire cellular estate with superior visibility, security, and control.

- **SIM Activation:** The agency deploys routers and other devices with both FirstNet® or Zscaler SIMs (or in tandem for the best resilience and coverage).
- **Network Integration:** Zscaler acts as the secure gateway for both SIMs. Traffic does not hit the open internet; it is routed directly to the Zscaler Cloud.
- **Zero Trust Enforcement:** The Zero Trust Exchange verifies the identity and context of the connection—not just the IP address.
- **Secure Access:** The connection is brokered to the specific application (Private Workload or SaaS) needed. The device is never placed on the network, preventing lateral movement if a device is compromised.

Business Values

Value pillar	What it means for agency operations (Chief / Ops / IT)	What it means for CIO/CISO (risk / security / architecture)
Mission continuity under incident conditions	Fewer disruptions to CAD/PTT/ROIP/ video during congestion, coverage shifts, and damaged infrastructure	Reduced outage risk from brittle gateways and single points of failure; improved resilience posture
Consistent policy across any cellular path	Same access experience and controls whether on primary or failover network; fewer "workarounds" in the field	Eliminates security gaps during failover; uniform enforcement and auditability
Reduced edge exposure	Less operational impact from compromised vehicle routers/IoT; safer expansion of connected assets	Reduced inbound exposure patterns; smaller attack surface and blast radius
Simplified operations and faster troubleshooting	Central visibility and fewer moving parts vs. multiple APNs/VPNs/tool sprawl	Centralized logging/telemetry supports incident response, governance, and control validation
Architecture efficiency	Less dependence on backhauling traffic and scaling legacy VPN infrastructure	Lower reliance on VPN concentrators; cleaner path to Zero Trust modernization and cost control
Compliance support (CJIS-sensitive workflows)	More consistent protection for sensitive data across vehicles, command posts, and mobile sites	Stronger evidence for compliance through consistent controls and logs (aligned to agency requirements)

Joint Architecture

The Power of Dual SIM: Assured Connectivity

The unique value of this partnership lies in the Dual SIM configuration, providing first responders with the “best of both worlds” in a single ruggedized router with all traffic routed through the Zscaler Zero Trust Exchange for protected access to mission critical applications.

1. Primary Slot: AT&T FirstNet® SIM (Assured Emergency Connectivity)

Role: The primary lane for mission-critical traffic.

Value: Provides FirstNet®’s “always-on” priority and preemption, ensuring first responders never compete with commercial traffic during emergencies or large-scale public events.

Integration: Connects via the Zscaler Cellular Partner Service on-ramp, extending Zero Trust inspection and enforcement to the FirstNet® core.

2. Secondary Slot: Zscaler Cellular SIM (3-Carrier Failover)

Role: The ultimate safety net.

Value: Provides automatic failover to 3 commercial carriers (Verizon, T-Mobile, AT&T Commercial). If the primary network is physically obstructed or unavailable in a remote location, the Zscaler SIM instantly routes traffic through the strongest available signal.

Integration: Delivers a unified Zscaler Cellular Service, managed entirely by Zscaler, ensuring the device remains protected even when off the FirstNet® network.

One Mission, Unified Policy

Whether traffic is traversing the FirstNet® band 14 or a commercial fallback network, Zscaler ensures the security posture remains identical.

Key Use Cases for Public Safety

1. Connected Emergency Vehicles

Challenge: Patrol cars and fire trucks move through dead zones and congested urban areas, often losing VPN connections to CAD, situational awareness application, and ROIP.

Solution: A Dual SIM setup ensures the vehicle is always connected. High-priority traffic uses FirstNet®, while the Zscaler SIM stands by to bridge any coverage gaps.

Outcome: Officers retain constant access to license plate readers, body cam uploads, and dispatch data without manual intervention.

2. Mobile Command Centers & Disaster Response

Challenge: Establishing secure connectivity immediately upon arrival at a disaster site where infrastructure may be damaged.

Solution: Zscaler Cellular creates an instant “Zero Trust zone” around the command post.

Outcome: Agencies can securely share data with federal and local partners without exposing the internal network or any VPN endpoints, ensuring interoperability during multi-agency responses.

3. Secure Radio-Over-IP (ROIP)

Challenge: Legacy radios are being replaced by LTE-enabled PTT (Push-to-Talk) devices that require low latency and high security.

Solution: Zscaler prioritizes voice traffic through the Zero Trust Exchange, preventing jitter and ensuring encrypted communication channels cannot be intercepted.

Outcome: Unprecedented resilience and security for mission critical voice traffic.

Conclusion

Zscaler helps first responders maintain secure, uninterrupted access to mission-critical applications—CAD, ROIP/PTT, video, and situational awareness—even through congestion and network transitions. By enforcing Zero Trust access with consistent policy and visibility across cellular paths, agencies can reduce reliance on brittle VPN choke points, shrink edge exposure for vehicle/IoT infrastructure, and improve mission assurance under emergency conditions.

Talk to Zscaler Sales to request a demo and see how Zscaler Cellular can strengthen mission assurance for first responders.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Experience your world, secured.™