

Dejero

Beyond Bonding

Redefining Mission-Critical Connectivity

June 2026

Dejero

Copyright © 2026 Dejero Labs Inc. Dejero, Smart Blending Technology, and the Smart Blending Technology logo are trademarks or registered trademarks of Dejero Labs Inc. All other trademarks are the property of their respective owners. Design, features, and specifications are subject to change without notice. D-WP-107-001

connect@dejero.com

+1 519 772 4824

dejero.com

Table of Contents

Executive Summary 4

The Critical Connectivity Landscape 4
- The Scale of Modern Requirements 4
- The Limitations of Traditional Approaches 4
- The "Failover" Gap: The Silent Killer of Operations 5
- Why Hybrid Networks Change Everything 5

Technical Architecture: *Smart Blending Technology* 6
- Deployment Architecture 6
- Connection Profiling and Management 7
  - Real-Time Performance Monitoring 7
  - Dynamic Connection Management 7
- Bufferbloat Management 8
- Flow and Application Acceleration 8

The Evolving Satellite Landscape: From Backup to Blended 10

Introducing the Dejero TITAN Family 12

Putting TITAN Command to the test 13
- Latency Comparison: Blending Advantage During Motion 14
- Rural Uptime Comparison: Blended vs Individual Carriers 14
- Blended Upload Throughput Analysis: Metro Atlanta 15

Security and Compliance Considerations 16
- Encryption and Data Protection 16
- FedRAMP Compliance 16
- Management and Visibility 17

Conclusion: Your Lifeline to Mission Success 17

References and Sources 18

Executive Summary

For public safety and defense operations, connectivity isn't a convenience; it's the difference between mission success and failure. Traditional network aggregation was built for static locations and predictable conditions—a world that doesn't exist on the modern battlefield or in emergency response.

This white paper explores **Dejero *Smart Blending Technology™*** and the **TITAN product family**. Unlike traditional failover systems, we intelligently optimize every packet across multiple network paths simultaneously. The result is a single, virtualized "super-pipe" that is unbreakable, providing the foundational strength required for Joint All-Domain Command and Control (JADC2) and high-stakes public safety missions.

The Critical Connectivity Landscape

A joint task force is coordinating disaster response across three states. Real-time video feeds from aerial drones need to reach command centers instantaneously. Ground units require persistent situational awareness. Medical teams are transmitting patient data to remote specialists. And all of this is happening in an environment where commercial networks are stressed, infrastructure may be damaged, and conditions are changing by the minute.

This isn't a hypothetical scenario, it's the reality defense and public safety organizations face every day. And traditional connectivity solutions simply aren't built for it.

The Scale of Modern Requirements

The numbers tell a compelling story. According to AT&T's Q4 2024 reporting, FirstNet, the nationwide public safety broadband network, now supports more than 7.8 million connections for over 30,600 public-safety agencies across the United States. The FirstNet Authority has committed over $8 billion to network evolution, including $6.3 billion for a standalone 5G core dedicated to public safety communications.

The Limitations of Traditional Approaches

Most connection aggregation technologies were developed for enterprise environments with fixed locations and wired broadband. They work reasonably well in controlled conditions but fall short when you introduce the variables that define public safety operations: mobility, harsh environments, unreliable networks, and the absolute requirement for zero downtime.

Traditional bonding solutions typically keep data flows "sticky" to a single connection. It's simpler to implement, sure. But this approach means you're never fully utilizing all your available bandwidth.

Worse, when a connection fails, and in the field, connections fail, you experience disruption. Flows terminate. Sessions timeout. Critical communications drop.

For a video conference in a corporate office, that's an inconvenience. For a field commander making time-critical decisions, it's unacceptable.

The "Failover" Gap: The Silent Killer of Operations

Most mobile routers rely on a sequential failover model but that approach creates a critical "gap" in situational awareness:

- **Disruptive failover:** A single SIM, or dual-SIM is only a single connection; when it fails, the system "hunts" for an alternate carrier, causing a hard failover that terminates flows and drops critical communications.
- **Bars don't equal bandwidth:** Seeing a cell tower does not guarantee bandwidth. In field tests, traditional connections were visible but unable to provide throughput when needed.
- **Idle Resource Drain:** Agencies often pay for 2, 3, or 4 idle carrier contracts that sit dormant, waiting for a primary failure. This passive model is both expensive and obsolete.

Why Hybrid Networks Change Everything

To meet modern operational requirements, defense organizations increasingly depend on wireless technologies, 4G/LTE, 5G, satellite, and Wi-Fi. These connections offer the flexibility and reach that fixed infrastructure can't provide. But they also introduce significant challenges. Wireless networks exhibit dramatically different characteristics than wired connections.

Bandwidth fluctuates based on congestion, distance from towers, and environmental conditions. Latency varies unpredictably. Packet loss occurs more frequently. And perhaps most critically, upload and download speeds are often highly asymmetric, a factor that traditional bonding solutions handle poorly.

For mobile and nomadic operations, vehicles, forward operating bases and field teams, the aggregated connection might depend entirely on these variable wireless technologies. You need solutions specifically engineered for this reality.

Technical Architecture: *Smart Blending Technology*



When Dejero developed *Smart Blending Technology*, the team started with a fundamental question: What if we stopped treating connections as static resources and instead managed them dynamically, in real-time, at the packet level?

The answer led to an approach that differs fundamentally from traditional solutions. Instead of assuming connections have fixed characteristics and keeping flows sticky to assigned links, *Smart Blending Technology* continuously measures connection performance and intelligently splits data across multiple paths on a packet-by-packet basis.

Deployment Architecture

The Blending architecture consists of two main components working in concert:

1. **Remote Endpoint:** A Dejero device is deployed at a field location, whether a branch office, mobile command vehicle, forward operating base, or nomadic deployment site
2. **Concentrator:** Working in conjunction with Dejero Control, our cloud-based management service, the Concentrator is implemented as a containerized and orchestrated cloud-based offering for high reliability

The Dejero device supports multiple links and creates a tunnel through each link between the device and the Concentrator. IP packets are split, during segmentation and reassembly, working independently in each direction. Network address translation assigns an IP belonging to the Concentrator before egressing to the Internet, allowing flows to remain unbroken even if links fail or change IP addresses.

Small deployments can leverage Dejero for all edge functionality. The router directs traffic either through the VPN tunnel or directly to the Dejero device based on routing tables, while the network aggregation function handles splitting traffic over available connections.

For large/enterprise deployments using routers or SD-WAN appliances behind Dejero gain the best of both worlds: Dejero provides effective, efficient, high-performance blending of connections with potentially different characteristics, while the SD-WAN manages higher layer functionality and security between locations.

Connection Profiling and Management

Achieving high performance while avoiding the issues limiting other solutions demands meeting particular technical requirements. The blending profiling system continuously monitors each network's characteristics, including throughput, latency, and packet loss, in real-time.

Real-Time Performance Monitoring

This feedback loop allows both the Dejero device and the Concentrator to operate with fine granularity as they determine the best link over which to send each packet. The system blends connections independently in both transmit and receive directions. Unlike traditional load-balancing solutions that force return traffic onto the same link used for the original IP flow, it makes no assumption of symmetrical performance, critical in access networks where download capacity typically exceeds upload capacity.

Importantly, data usage for these real-time insights is minimized by "piggybacking" measurement on top of application data wherever possible. If a connection lacks sufficient application data to properly characterize performance, data is adaptively incorporated to ensure persistent performance monitoring.

Dynamic Connection Management

By statistically filtering real-time measurements, Dejero *Smart Blending Technology* assesses network performance and reliability.

This approach allows connections to be added dynamically without reconfiguration or manual calibration. As soon as a connection is observed by the system (link status up, IP address assigned), *Smart Blending Technology* begins probing to assess performance and reliability, then automatically adds it to the blending pool when it will provide benefit.

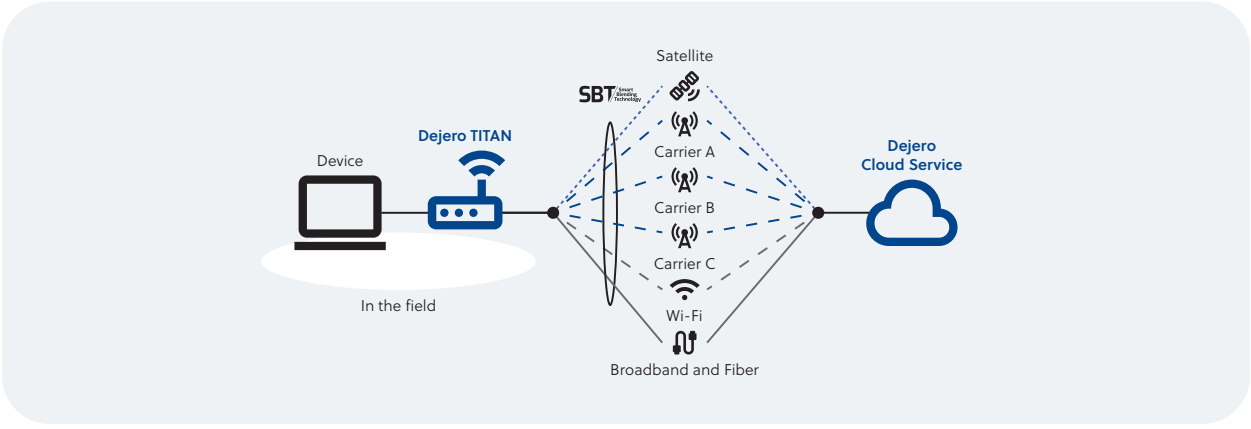


Figure 1 — Dejero *Smart Blending Technology* deployment architecture

Bufferbloat Management

Buffering is normal network behavior, allowing resources like routers, CMTS systems and OLTs to gracefully handle traffic bursts by increasing latency slightly rather than dropping packets. However, excessive buffering (bufferbloat) leads to high latency as queues fill and, ultimately, causes packet drops.

Bufferbloat occurs when a sender sustains transmission through the connection buffer faster than the buffer's drain rate, causing the buffer to completely fill. This fills the output queue of network resources, leaving a standing buffer even after the sender backs off, in extreme cases, packets are dropped at the buffer input.

Most connection aggregation algorithms don't explicitly target bufferbloat, instead relying on other system components to handle it (if at all). In contrast, Dejero *Smart Blending Technology* detects and actively reduces bufferbloat, critical to preserving performance when other system components cannot.

Smart Blending Technology employs two complementary approaches:

- **When the device is the bottleneck:** Per-flow active queue management (AQM) techniques distinguish between "good" queues (temporary queues from traffic bursts) and "bad" queues (standing queues that never clear). Bad queue packets are dropped, providing feedback to senders. Flows that don't respond (relentless senders) are segregated so they don't introduce latency to other flows.

- **When links are the bottleneck:** A rate-based congestion control algorithm with feedback ensures link latency stays close to base propagation delay.

Flow and Application Acceleration

When TCP and UDP flows are split across connections with different properties, congestion control algorithms introduce complexities that can inadvertently undermine performance. Dejero *Smart Blending Technology* incorporates accelerators that act on flows/applications or classes of applications to address these issues.

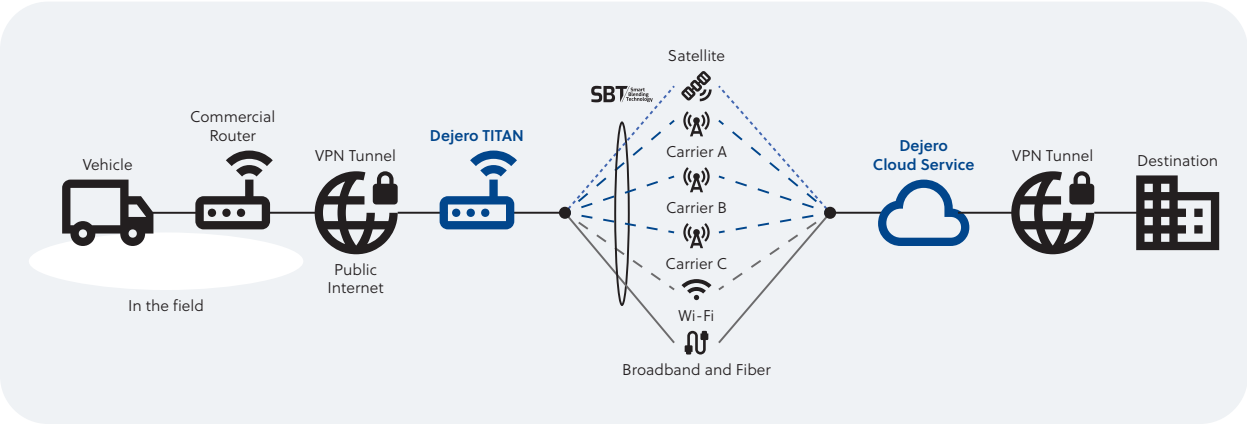


Figure 2 — Typical Dejero *Smart Blending Technology* deployment with external commercial router

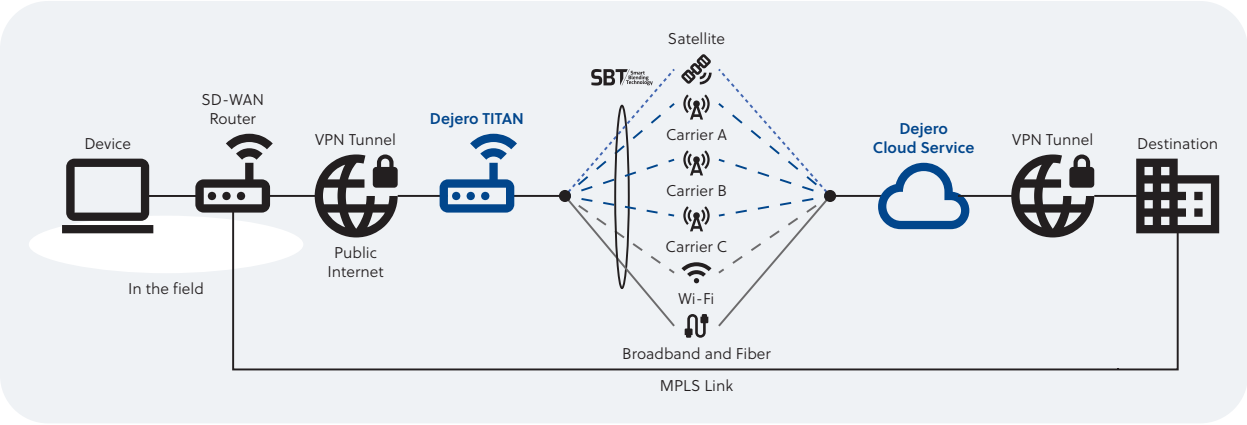


Figure 3 — Dejero *Smart Blending Technology* integrated with existing SD-WAN

TCP flows are accelerated using transparent proxying techniques. The TCP flow is terminated just before splitting occurs; the accelerator acknowledges data from the sender on behalf of the ultimate destination, then ensures reliable transmission over blended links. The sender's congestion control algorithm never sees premature indications of reaching link capacity.

For live video contribution and distribution, applications that traditionally demanded large-capacity MPLS links for reliable transmission, *Smart Blending* adaptively trades off latency to add tighter jitter control and packet recovery (ARQ) when transmitting over potentially unreliable public Internet links. The application experiences a more stable connection; the tradeoff of slightly higher latency is acceptable for video scenarios where two-way interactivity isn't required.

Note: In November 2018, Dejero was recognized with a prestigious Technology & Engineering Emmy® Award for "excellence in engineering creativity," honoring a decade of achievements in the field of live transmission.



Competitors Sell	Dejero Delivers
Failover + Session switching	Simultaneity + Packet-level blending
Single points of failure + Transport lock-in	Zero-blip resilience + Transport agnosticism

The Result: A single, virtualized "super-pipe" that's unbreakable, and sovereign.

Figure 4 — Dejero *Smart Blending Technology* comparison

The Evolving Satellite Landscape: From Backup to Blended

For years, satellite connectivity in defense and public safety was treated as a last resort, a contingency link activated only when all else failed. That calculus is changing rapidly, and Dejero *Smart Blending Technology* is built for where the satellite industry is heading, not just where it is today.

The proliferation of Low Earth Orbit (LEO) satellite constellations has fundamentally altered the performance equation. Where traditional Geostationary Earth Orbit (GEO) satellite links carried latencies measured in hundreds of milliseconds, a significant constraint for real-time communications, modern LEO systems operate at orbital altitudes that bring latency into a range increasingly comparable to congested terrestrial cellular. For mobile and nomadic operations in challenging environments, this shift opens satellites up as an active, always-on participant in the connectivity mix rather than a dormant fallback.

At the same time, Non-Terrestrial Network (NTN) standards, including direct-to-device (D2D) capabilities being developed under 3GPP's Release 17 and beyond, are beginning to blur the line between cellular and satellite entirely. In environments where terrestrial towers are damaged, destroyed, or deliberately avoided for operational security, these emerging standards allow satellites to serve as a seamless extension of the cellular fabric. Field units will eventually carry devices that connect to the best available signal, ground tower or satellite constellation, without any manual intervention or mode switching.

This is precisely the environment Dejero *Smart Blending Technology* was designed to thrive in.

Because this technology operates at the packet level, managing every path independently and in real time, it makes no assumption about the type of network a given connection represents.

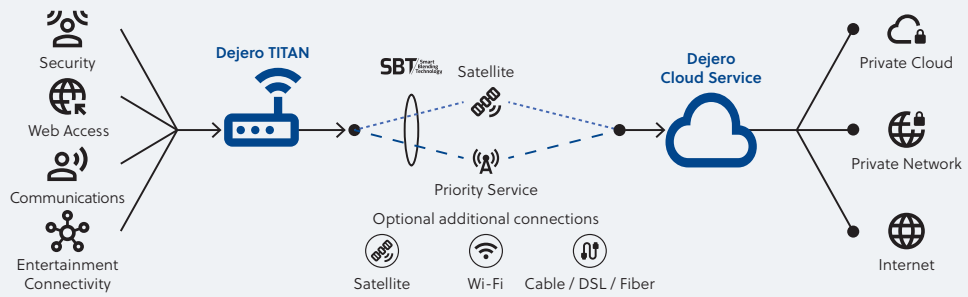


Figure 5 — A Dejero *Smart Blending Technology* deployment flow

A Starlink terminal in the field is treated the same way as an LTE modem: continuously profiled for throughput, latency, and reliability, and assigned traffic accordingly. When a satellite offers the best available path, or the only available path, *Smart Blending* routes through it without disruption. When terrestrial connections recover or become available, satellite capacity is automatically redistributed, not abandoned.

This architecture also addresses one of satellite's persistent technical challenges in a blended environment: asymmetry. Satellite links, particularly LEO systems, often exhibit significantly different upload and download characteristics depending on orbital geometry, beam congestion, and atmospheric conditions. As detailed earlier in this paper, *Smart Blending Technology* makes no assumptions about connection symmetry, a critical design decision that allows satellites to contribute meaningfully in both transmit and receive directions rather than being artificially constrained by algorithms built for balanced wired links.

Looking ahead, the convergence of 5G, NextG infrastructure, LEO expansion, and D2D satellite access will create a connectivity environment of unprecedented density and complexity. Organizations that lock themselves into single-technology architectures today will face costly rearchitecting as the landscape evolves. *Smart Blending's* carrier-agnostic, technology-agnostic design means Dejero TITAN platform deployments are positioned to absorb these advancements automatically, each new satellite provider, each new spectrum band, each new NTN capability becomes an additional path that our technology can blend rather than a replacement system that requires forklift investment.

The satellite space is no longer a static backup tier. It is becoming a dynamic, high-performance layer in the hybrid-path connectivity stack. *Smart Blending Technology* ensures that Dejero TITAN users are ready for it, today and as the constellation ecosystem continues to mature.

Introducing the Dejero TITAN Command



Figure 6 — Dejero TITAN Command

Dejero *Smart Blending Technology* has powered mission-critical communications for nearly two decades. Now, we're taking it to the next level with the Dejero TITAN product family, a comprehensive portfolio engineered to deliver foundational network strength across every deployment scenario.

Dejero TITAN Command is the first release of this product line. It's the world's first triple 5G connectivity platform, featuring three independent Telit FN990A40 5G/LTE advanced modems with integrated antennas, GPS/GNSS, and *Smart Blending Technology*.

Three completely independent cellular paths, each capable of connecting to different carriers, all being intelligently blended at the packet level. If one modem fails, you have two more. If a carrier experiences an outage, traffic routes through the others. The redundancy is unprecedented.

TITAN Command specifications designed for defense requirements:

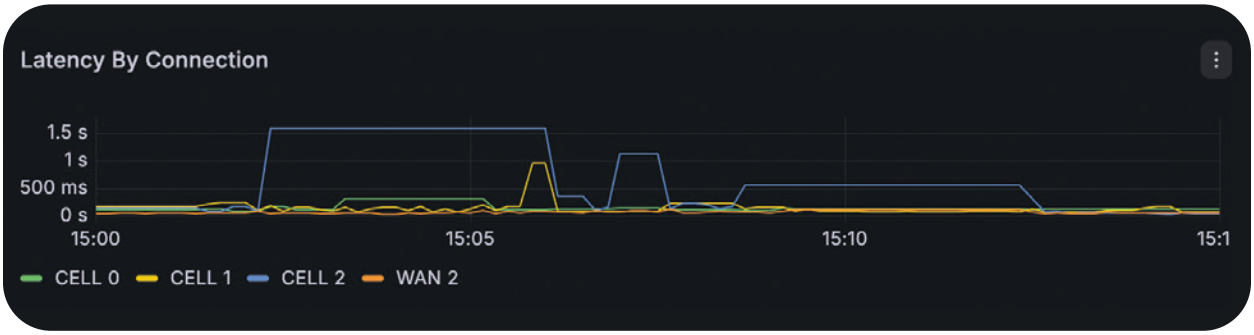
- **Operating temperature:** -40°C to 70°C (-40°F to 158°F), tested to MIL-STD-810G for shock and vibration
- **Form factor:** Compact laptop-size (6.0 x 32.8 x 25.7 cm) with 14 integrated high-gain antennas
- **Connectivity:** Four 2.5 Gigabit Ethernet ports, Wi-Fi 6 support, high-precision GPS/GNSS with ADR & UDR synchronization
- **Power:** PoE++ input (802.3bt Type 4), 8-36V DC input, or AC adapter, flexible deployment options
- **Compute:** High-performance Intel processor with 128GB eMMC storage
- **Environmental:** Fanless design for silent operation with optional enclosures including IP67 rated dust and water resistance

Putting TITAN Command to the Test



Data analysis (November, 2025) from a 640-mile road test, from Memphis, TN to Savannah, GA, conducted by Dean Taylor, Director of Technical Account Management at Dejero. Data findings illustrate the performance chasm between traditional, legacy dated solutions and Dejero technology.

Metric	TITAN Command	5G Competitor
Connectivity model	Simultaneous blending	Sequential failover
Upload throughput	Consistently high >50+Mb/s	Dropped to <1Mb/s
Data continuity	Zero drops over 640 miles	Frequent “hard” session resets
Redundancy	3x independent 5G modems	Dual-radio with standby

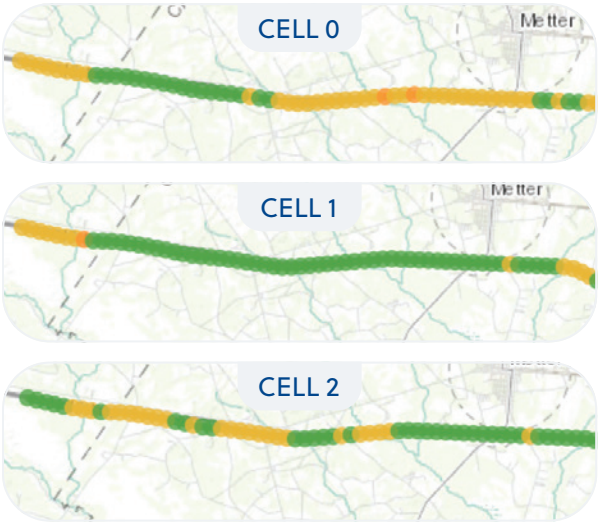


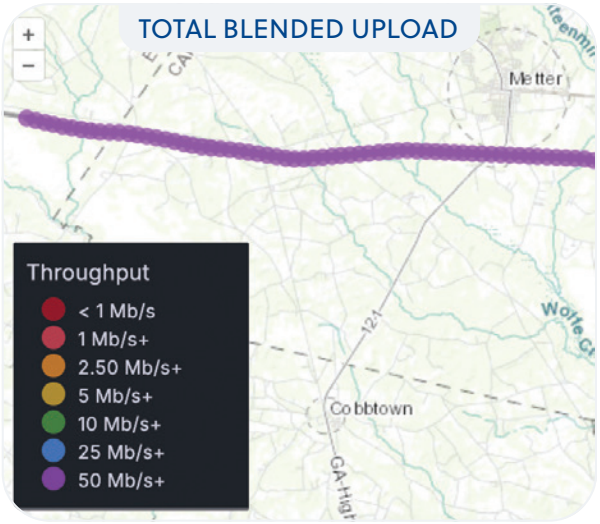
Latency Comparison: Blending Advantage During Motion

120ms effective average — better than slowest connection (CELL 2: 1,865ms) and more stable than fastest (CELL 1: 72ms but spikes to 1,865ms).

Key Advantage: Spike Mitigation. When CELL 2 spiked to 1.865 seconds at 1502 CT — **undesirable for real-time apps** — the blended connection absorbed this by intelligently routing through CELL 0/2/WAN 2, keeping effective latency at 524ms peak (71% reduction).

Motion Impact: In a moving vehicle, individual connections experience handoffs, signal fading, and satellite reacquisition. *Smart Blending* dynamically shifts traffic to lowest-latency paths, preventing any single connection's degradation from affecting user experience. No reliance on one unstable link.





Rural Uptime Comparison: Blended vs Individual Carriers

2.6x Reliability Improvement: Blended (98%) vs. worst single carrier CELL 0 (35%) - even when one carrier fails frequently, service continues.

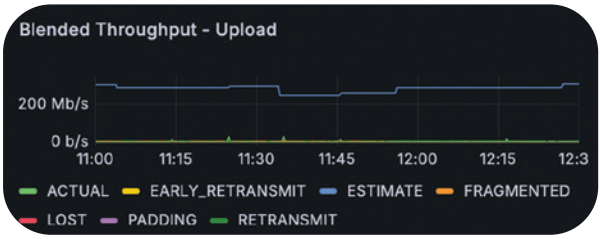
1.6x vs Best Carrier: Blended (98%) vs. best single carrier CELL 2 (58%) - blending eliminates individual carrier intermittency.

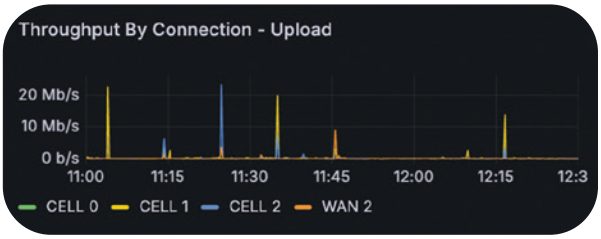
Zero Complete Outages: When CELL 1 dropped offline after 1555 CT, CELL 0 and CELL 2 maintained service. No period had all three carriers down simultaneously.

The blended connection achieved near-continuous service (98% uptime) despite the best single carrier never exceeding 58% individual availability.









Blended Upload Throughput Analysis: Metro Atlanta

250 Mbps
entering Douglas County at 1234 ET

309 Mbps
leaving metro area at 1329 ET

1. **Urban Network Congestion**
   The vehicle traveled through Metro Atlanta (lat 32.5°N → 34.9°N) during midday. Dense urban areas have higher cellular user density, causing tower congestion. All three CELL connections degraded simultaneously, suggesting shared network load rather than signal issues.

2. **Frequent Cell Tower Handoffs**
   Moving at ~23 mph in stop-and-go traffic through the metro area requires constant handoffs between towers. Each handoff temporarily reduces throughput during re-authentication. Carrier A showed 46% data gaps, Carrier B had 72% gaps—indicating connection interruptions during handoffs.

3. **Building/Terrain Interference**
   Metro Atlanta's high-rise buildings create signal blockage. RSRP remained decent (-87.6 dBm avg for Carrier A) but Carrier C degraded to -116 dBm floor, showing physical obstruction impacts. Urban canyons reduce line-of-sight to towers.

4. **WAN Connection Degradation**
   (WAN 2, <5 Mbps) may have experienced satellite reacquisition delays during building shadowing.

Metro Atlanta Travel Summary: *Smart Blending* throughput maintained 220+ Mbps despite individual link failures. Without blending, service would've been unusable when any single connection failed.

Security and Compliance Considerations

Defense and government organizations don't just need reliable connectivity, they need secure, compliant connectivity. We've designed the Dejero TITAN platform with these requirements in mind from the ground up.

Encryption and Data Protection

All traffic between TITAN devices and the Dejero Control cloud service is encrypted. The system supports integration with existing VPN infrastructure, allowing organizations to extend their security policies to edge connectivity. Network Address Translation ensures that internal addressing remains hidden from external networks.

FedRAMP® Compliance

Dejero Control and Concentrator has achieved **FedRAMP Moderate authorization**, with U.S. Customs and Border Protection (CBP), a component of the Department of Homeland Security, serving as the sponsoring agency. This authorization confirms that Dejero's cloud-based management and connectivity platform meets the rigorous security controls required for processing federal information, including controlled unclassified information (CUI), in government systems.

Dejero Control and Concentrator is now listed on the FedRAMP Marketplace and available for immediate federal agency deployment.

Because FedRAMP authorization is reusable, any federal agency can leverage the existing authorization package without duplicative security assessments, significantly accelerating procurement timelines.

The authorization encompasses more than 300 continuously monitored security controls, providing ongoing assurance, not just a point-in-time assessment. The containerized, orchestrated architecture of the Dejero cloud service supports the access control, audit logging, and incident response requirements that federal procurement and security teams require.

For Dejero TITAN deployments, this means agencies gain a fully authorized management backbone from day one. TITAN Command devices are centrally administered through Dejero Control, giving federal administrators a single, FedRAMP-authorized pane of glass for device configuration, real-time network monitoring, bandwidth management, and fleet-wide operational continuity, all within a security posture already validated for government use.

Combined with FirstNet®, Verizon Frontline integration and T-Mobile T-Priority, the Dejero platform delivers an end-to-end connectivity and management solution engineered to meet the compliance, security, and operational requirements of public safety and defense agencies. For more information, visit **dejero.com/fedramp**.

Management and Visibility

Dejero Control provides centralized visibility across all deployed devices. Administrators can monitor connection status, bandwidth utilization, and system health in real-time. RESTful APIs and SNMP v3 support enable integration with existing network management and security information systems.

Management capabilities include:

- Web-based management interface for device configuration
- Multi-color LED status indicators for visual monitoring
- Real-time bandwidth and latency monitoring per connection
- Fleet-wide deployment management through Dejero Control

Conclusion: Your Lifeline to Mission Success

Smart Blending Technology embodies Dejero's belief that one connection is never enough. By measuring and adapting to network conditions in real-time, by splitting data intelligently at the packet level, by managing the complexities of asymmetric wireless connections, we deliver connectivity that just works, even when nothing else does.

The Dejero TITAN product family brings this technology to public safety, defense and emergency response agencies in purpose-built form factors with the certifications and environmental specifications these demanding applications require.

When lives depend on connectivity, when mission success requires communications that cannot fail, when you need reliable connectivity anywhere. That's what Dejero delivers.

Your mission is too important for anything less.

Learn More

To explore how Dejero TITAN can support your mission-critical connectivity requirements:

Visit: **dejero.com/titan**
Email: **connect@dejero.com**
Call: +1 519 772 4824

References and Sources

The statistics and information in this white paper are drawn from the following publicly available sources:

- FirstNet Authority, "FirstNet in 2024: A Year of Growth, Innovation, and Bold Plans for the Future," firstnet.gov, December 2024
- Urgent Communications, "FirstNet tops 7.8 million connections, 30.6K agencies," urgentcomm.com, Q3 2025
- U.S. Department of Defense, "Summary of the Joint All-Domain Command & Control (JADC2) Strategy," media.defense.gov, March 2022
- Executive Gov, "DOD Approves Private 5G Network Deployment Strategy," executivegov.com, November 2024
- Breaking Defense, "The Pentagon's fiber future: How DoD networks race to meet new demands," breakingdefense.com, November 2025
- Federal Communications Commission, "Spectrum Rules and Policies for the Operation of Unmanned Aircraft Systems," FCC 24-91, August 2024
- Defense One, "Connectivity at the Core: Resilient Communications are Critical to Realizing JADC2," defenseone.com, April 2024
- Dejero, "Dejero Control Achieves FedRAMP® Moderate Authorization," dejero.com, March 5, 2026.



Dejero

About Dejero

As organizations accelerate their digital transformation, they choose Dejero to solve the most challenging applications of live video and real-time data exchange over wireless IP networks.

Dejero delivers resilient, uninterrupted internet connectivity vital to critical communications and cloud access. It provides connection diversity, redundancy, and continuity by intelligently combining multiple networks into a single managed service.

connect@dejero.com
+1 519 772 4824
dejero.com

Whitepaper published: June 2026
Author: Matt Scully