Secure Your Operational Equipment with Zero Trust: The Smarter Alternative to VPNs and Private APNs

Richard Reisbick, CTO FreeWave

When it comes to remote connectivity for critical operational equipment, the stakes couldn't be higher. Compromised systems are becoming more prevalent and protection of your vital systems can prevent significant damage. Traditional VPNs and private APNs may provide connectivity, but they fall short on security, scalability, and ease of use—leaving your infrastructure vulnerable to breaches and inefficiencies. Enter FreeWave's **Secure Connectivity using Zero Trust (SCZT)**: A revolutionary approach, using Zero Trust Architecture, to secure, scalable, and cost-effective remote connectivity tailored for critical operations.

Why SCZT Is the Right Choice for Operational Equipment Connectivity

1. Maximize ROI While Reducing Risk

VPNs and APNs Come with Hidden Costs:
The upfront costs for deploying private APNs or VPNs for operational connectivity are high, and the ongoing maintenance costs add up quickly—$30,000+ annually for medium-sized operations. More importantly, a single infiltration could cost millions in downtime, lost productivity, and breach recovery (average breach cost: $4.45 million).

SCZT Offers Superior ROI:
By replacing VPNs or private APNs with Zero Trust, you can reduce total cost of ownership by 40–60% over five years. Automation, cloud-native infrastructure, and simplified management drive cost savings while significantly lowering the risk of catastrophic breaches.

2. Bulletproof Security for Critical Equipment

The Problem with VPNs and APNs:
Both VPNs and APNs rely on implicit trust, meaning once authenticated, users or devices are granted broad access to the network. This

makes them vulnerable to credential theft, insider threats, and lateral movement by attackers.

The SCZT Advantage:
With micro-segmentation, Zero Trust isolates access to specific equipment or systems, ensuring that even if a user or device is compromised, the rest of your operational environment remains safe. Continuous verification and least-privilege access protect critical assets from malicious actors.

3. Simplified Connectivity with Better User Experience

VPN and APN Challenges:
VPNs introduce latency and can slow down data transfers, particularly in industrial or operational environments where low latency is critical. Private APNs require complex setup, carrier management, and are costly to scale for global operations.

SCZT Simplicity:
Zero Trust enables direct-to-device or direct-to-app connectivity, bypassing the bottlenecks and latency issues of VPNs. With real-time policy enforcement, remote workers and systems connect securely and efficiently to only what they need—without impacting performance or scalability.

4. Micro-Segmentation: Protect Every Piece of Your Operational Network

VPN/APN Weakness:
Once a VPN or APN connection is compromised, attackers can move freely across your entire network, targeting critical operational systems or data.

SCZT Micro-Segmentation:
Zero Trust creates isolated «segments» for each piece of operational equipment, limiting access on a per-device or per-application basis. This means:

Even if one segment is breached, the rest of your network remains secure.

Equipment and systems are protected against lateral movement by attackers.

Access policies can be tailored to specific roles, users, or devices.

Real-World Savings and Security

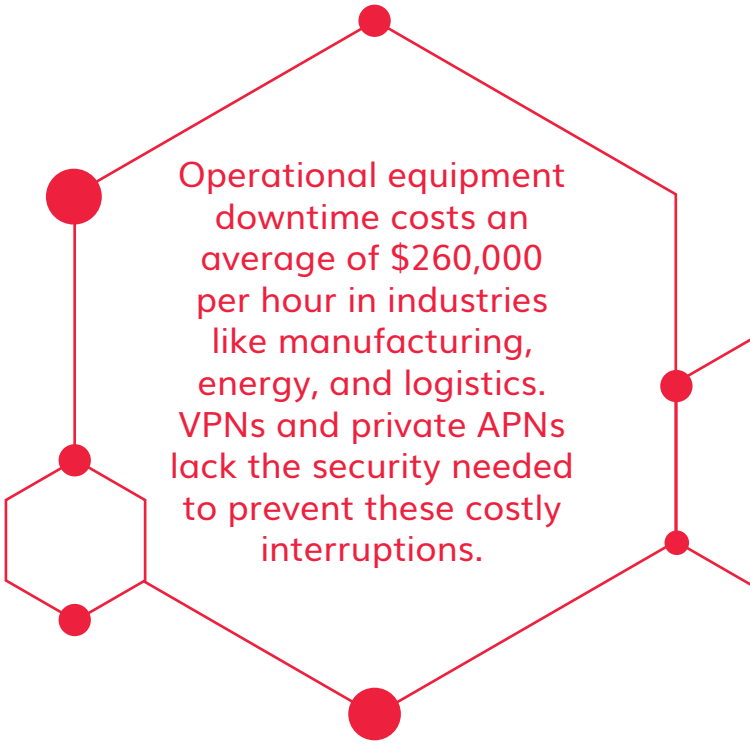
Breaches in Operational Systems Are Devastating

Operational equipment downtime costs an average of $260,000 per hour in industries like manufacturing, energy, and logistics. VPNs and private APNs lack the security needed to prevent these costly interruptions.

SCZT Delivers Results:
By preventing breaches and enabling faster recovery from incidents, Zero Trust reduces downtime risk by up to 70%. The combination of lower maintenance costs, stronger security, and improved user experience drives long-term savings and operational efficiency.

Ease of Transition

FreeWave's SCZT doesn't require a complete overhaul of your existing systems. It integrates seamlessly with your current infrastructure, enabling a phased and cost-effective transition from VPNs or private APNs.



FREEWAVE

FreeWave's SCZT is easily scalable using FreeWave's hardware or your own hardware. Utilizing a downloadable agent and our management platform it's scalable for global operations, whether you're securing one device or a worldwide network of critical equipment.

The Future of Remote Operational Connectivity

Switching to SCZT isn't just an upgrade—it's a necessity for modern, secure, and scalable connectivity.

Key Benefits at a Glance

- 70% fewer breaches = millions saved in downtime and recovery costs.
- 40–60% lower total cost of ownership compared to VPNs or private APNs.
- Seamless, direct connectivity for better performance and lower latency.
- Unmatched security through micro-segmentation and continuous verification.

Take Action Now

It's time to leave the outdated VPNs and private APNs behind. Replace them with Zero Trust and enjoy stronger security, higher ROI, and simplified connectivity for your critical operational equipment.

CONTACT US TODAY →

Protect your critical operations. Reduce risk. Improve efficiency.

Secure Connectivity using Zero Trust: The smarter, safer way to secure your operations.

FREEWAVE

FreeWave Technologies, Inc.
5395 Pearl Parkway, Boulder, CO 80301
866.923.6168 info@freewave.com

Made in the U.S.A. www.freewave.com