NETWORK INNOVATIONS

ARGUS ENTERPRISE

SECURED UTILITIES

Private Networks with Zero Trust Architecture Built for Operational Networks

THE CHALLENGE Public Networks and Legacy Trust Are No Longer Viable

Utilities organizations are modernizing their grids with smart meters, distributed energy resources (DERs), automation, and remote workforce tools; however, these efforts can expose your company to undesirable risks:

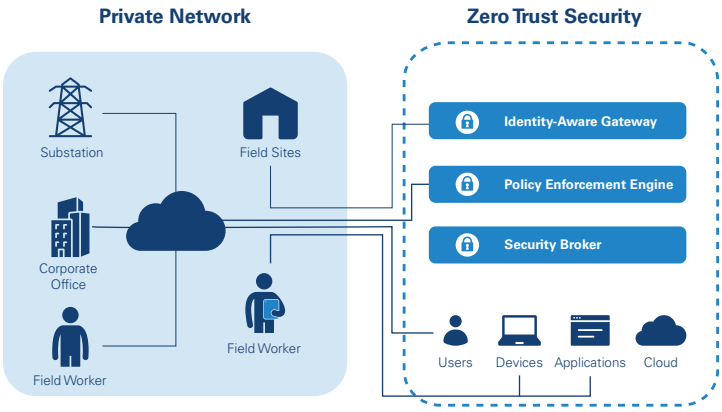
- Public carrier networks introduce latency, reliability, and security concerns
- Flat, perimeter-based network models allow lateral movement if breached
- Cyber threats targeting critical infrastructure are increasing in frequency and sophistication (e.g., ransomware, state-sponsored)

THE SOLUTION Combining Private Networks with a Zero Trust Overlay

The combination of a dedicated private network and Zero Trust security mitigates these risks by removing trust assumptions, enforcing access control, and securing communications end-to-end — from core to edge.

Private Networks (e.g., LTE, 5G, fibre) provide:

- Dedicated spectrum and bandwidth
- Low-latency, high-reliability links for SCADA, AMI, and control systems
- Operational control over performance, routing, and access
- Isolation from the public internet, enhancing protection



Zero Trust Architecture adds:

- Continuous verification of users, devices, and data flows — no implicit trust
- Micro-segmentation between IT, OT, and IoT/edge assets
- Policy-based access that dynamically adapts to risk and context
- Monitoring and auditability of every session, login, and connection attempt
- Together, they create a resilient, secure, and scalable communications fabric purpose-built for utility operations.

Together, they create a resilient, secure, and scalable communications fabric purpose-built for utility operations.

Real-World Applications

APPLICATION	VALUE OF PRIVATE & ZERO TRUST
Substation Automation	Secure, isolated control of IEDs, RTUs, sensors — with policy-based access by zone and role
AMI (Smart Metering)	Scalable metering network with Zero Trust enforcement at meter concentrators
Field Workforce Connectivity	Encrypted LTE/5G connections with identity-based access per technician
Renewable/DER Integration	Segmented access to distributed generation (solar, wind, EV chargers)
Grid Monitoring and Fault Detection	Real-time, secure telemetry backhauled on a trusted channel
Corporate-OT Integration	Enable SCADA-to-IT data flow securely via micro-segmented zones
Disaster Recovery/Black Start	Guaranteed comms even during public network outages or cyber incidents

Strategic Benefits for the Utility

- **Regulatory Compliance**: Supports CSA Z246.1, NERC CIP, and CER cyber requirements
- **Resilience and Business Continuity**: Maintains operations during internet outages or attacks
- **Threat Containment**: Prevents lateral movement through identity-based segmentation
- **Remote Ready**: Securely supports digital substations, mobile crews, remote diagnostics
- **Reduced Vendor Risk**: Limits contractor access to only authorized systems, times, and locations
- **Scalability**: Ready for cloud integration, DER growth, smart grid expansion

CONCLUSION

Deploying a private network with Argus Zero Trust is not just an IT initiative — it's a critical infrastructure investment. It ensures that the grid, the field, and the enterprise are.

About Network Innovations

Network Innovations is a global technology integrator that keeps people, places and things connected with always-available communications solutions anywhere in the world. Its customers operate in industries including government and defense, public safety, oil and gas, media, mining, utilities, recreation, and maritime. Established in 1989, Network Innovations is headquartered in Calgary, Canada, and employs over 250 industry experts across four continents.

Meeting Your Mission. With Passion.