

# Risks Utilities Face Without OT Visibility

Private LTE and 5G networks promise transformation, but without OT visibility, utilities risk grid instability, cyberattacks, and wasted investments.



NETSCOUT®

# Risks Utilities Face Without OT Visibility

## CONTENTS

Introduction .....3

Wireless Networks In Action.....4

NETSCOUT Delivers Observability .....6

Case Study:  
How NETSCOUT Helps Improve Performance And Security.....7

Observability Delivers Reliability .....8



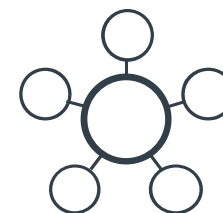
## Introduction

Utilities are modernizing their grids to meet evolving demands, and real-time visibility into their private wireless networks is critical for ensuring reliability, security, and efficiency. Without it, they face increased risks of service interruptions, cybersecurity threats, and regulatory penalties. While not limited to the utility sector, the growth of private LTE and 5G—reaching 4,700 deployments and a market value of \$1.8 billion in 2024—reflects increasing adoption across industries, including critical infrastructure like energy and utilities

While modernization is essential to support the clean energy transition, increased electric vehicle adoption, and challenges posed by extreme weather, reliability remains the top priority for utilities. To maintain uninterrupted operations, seamless wireless communication between operational technology (OT) networks, IoT devices, and field operations is imperative.

Many utilities are turning to private LTE and 5G networks to enhance operational control. In fact, global spending on private LTE and 5G infrastructure for sectors like energy, manufacturing, and transportation is projected to grow at a compound annual growth rate (CAGR) of approximately 20% between 2024 and 2027—surpassing \$6 billion by the end of 2027<sup>1</sup>. Some utilities rely on traditional carrier service providers for LTE connectivity, while others are investing in their own private networks. However,

<sup>1</sup>. Source: [ResearchAnd Markets.com](https://www.researchandmarkets.com)



To deliver rock-solid reliability, utilities must maintain uninterrupted wireless communication between their OT networks, IoT devices, and field operations.



managing these networks presents challenges, as many utilities lack the internal expertise to build, operate, and secure them effectively.

With real-time observability, utilities can minimize outages, strengthen cybersecurity, and navigate evolving regulations—ensuring the reliable service their customers depend on.

## Wireless Networks In Action

Utilities are implementing private LTE and 5G networks to gain greater control over their infrastructure, reducing their dependence on traditional carriers. If a provider's mobile network goes down during a national disaster, for example, a utility's ability to monitor its grid would be compromised when it is needed most. Relying on carrier networks becomes increasingly expensive as utilities expand their networks with more sensors and IoT devices—driving the need to explore private LTE and 5G solutions as a potentially more cost-efficient option.

As utilities build out their own wireless networks, however, they also must meet the challenges of managing those networks. They must ensure consistent, reliable wireless coverage across diverse and often remote geographies, acquire real-time visibility for effective troubleshooting, and implement effective security and compliance measures. For example, should a power line go down during a storm, a utility must cut off power



Cyberdefense becomes more demanding as utilities build out their OT networks and add sensors; as more of the OT network comes online, it expands the attack surface, making the utility more vulnerable to cyberattacks.



to the wire before it hits the ground—a feat that requires sub-second response times. Regulation requires that a utility have such capabilities, but reliability ensures that they will work when they are most needed: in bad weather and high-risk locations where connectivity may be challenging.

Running a wireless network also requires utilities to perform many tasks they might expect a service provider to handle, such as protecting the network from spam traffic, blocking basic cyberattacks, and preventing sophisticated DDoS attacks. Cyber security becomes more demanding as utilities build out their OT networks and add sensors; as more of the OT network comes online, it expands the attack surface, making the utility more vulnerable to cyberattacks.

Those in charge of operating the wireless network need new skills distinct from those needed to carry out the utility's core mission of delivering energy or electrical power. Utilities need highly trained experts like RAN engineers to build and maintain a wireless network to ensure constant visibility of network devices and traffic. However, hiring and training staff to manage wireless networks is not a trivial matter. Most utility IT and OT teams are already working full-time to support legacy systems and new technology rollouts.



NETSCOUT works as a trusted partner to provide real-time visibility and actionable insights, helping utilities make faster, data-driven decisions to reduce downtime, tighten security, and meet regulatory demands.



## NETSCOUT Delivers Observability

Utilities know that maintaining uptime, ensuring network performance, and defending against cyber threats are constant priorities. NETSCOUT works as a trusted partner to provide real-time visibility and actionable insights, helping utilities make faster, data-driven decisions to reduce downtime, tighten security, and meet regulatory demands. With NETSCOUT, utilities can confidently manage their networks, knowing they can quickly detect and mitigate risks before they impact operations.

NETSCOUT's observability and security solutions can help utilities maintain grid reliability, security, and compliance over their wireless network. This advanced level of observability gives utility leaders a uniform view of how their networks are performing and what disruptions may be looming.

Utilities need assurance of consistent uptime, low latency, and seamless connectivity for mission-critical applications. The data and insights NETSCOUT provides mean utilities can do all that while optimizing their wireless network performance, improving service reliability, preventing costly operational disruptions, and generating tangible ROI by reducing network downtime.

The same visibility that enables utilities to optimize OT performance powers real-time threat-hunting capabilities, enabling utility teams to identify unauthorized access and lateral movement in the event of a cyberattack. In addition, key security initiatives like North American Electric Reliability Corp. (NERC) Critical Infrastructure Protection (CIP) and zero-trust strategies become easier to implement when teams have access to more insightful data.





## How NETSCOUT Helps Improve Performance And Security

NETSCOUT's observability and cybersecurity solutions helped one U.S. utility detect and isolate a compromised network device, preventing data loss and reinforcing its zero-trust security strategy. In addition, the utility avoided regulatory scrutiny, mitigated financial risk from network disruptions, and upheld its commitment to reliable service.

The utility was dealing with intermittent latency and data loss across its substation networks. Commands to network devices were delayed, which increased the risk of service interruption. Traditional network monitoring tools couldn't penetrate encrypted traffic where the problem was and thus were ineffective at finding the root cause.

The utility partnered with NETSCOUT, enabling it to monitor problem connections, analyze live network traffic, and drill all the way down into the contents of network packets as needed. The utility was able to analyze live network traffic, detect anomalies, and correlate performance degradations with LTE spectrum congestion issues. They identified excessive retransmissions and congestion on specific LTE backhaul links, and were able to optimize Quality of Service (QoS) settings, prioritize the right types of traffic, and restore efficient grid communications. NETSCOUT made the problem clear and solvable by enabling the utility to drill deeper into the data than would have been possible using other solutions.

The same utility was able to thwart a cyber intrusion targeting its substation control systems with the assistance of NETSCOUT and its cybersecurity expertise. The utility's security team detected an unusual outbound traffic pattern from a field router, but traditional security tools did not identify it as a threat. NETSCOUT analyzed the traffic passing through the device at a deeper level, which showed that the router had been compromised and was exfiltrating data in microbursts to an unauthorized external IP address, a known tactic of nation-state actors utilized in operations like Volt Typhoon.

By correlating encrypted traffic patterns with indicators of compromise, NETSCOUT pinpointed the attack's origin and provided forensic evidence to help block the malicious activity before it could escalate.



## Observability Delivers Reliability

Utilities must continue to reliably deliver energy to their customers despite the challenges of grid modernization. As OT networks become more sophisticated and private wireless networks become more prevalent, utilities must rely on advancements in observability to ensure their operations are reliable, secure, and compliant. Because their customers expect nothing less.

**Learn how NETSCOUT can help utilities secure, optimize, and manage their private wireless networks.**

Contact us

**NETSCOUT**

NETSCOUT SYSTEMS, INC.® (NASDAQ: NTCT) delivers multi-purpose, real-time visibility, troubleshooting and protection wherever your technology infrastructure and business applications reside. NETSCOUT Smart Data gives technology and business teams the next-generation level of visibility to see the full range of performance, availability and security risks, earlier and with more precision, to resolve problems faster. That's why the world's most demanding government, enterprise and service provider organizations rely on NETSCOUT solutions to assure and protect the digital services which advance our connected world.

Visit [netscout.com](https://netscout.com) or follow @NETSCOUT on X, Facebook, or LinkedIn.

© 2025 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, the NETSCOUT logo, Omnis, Guardians of the Connected World, Adaptive Service Intelligence, Arbor, ATLAS, InfiniStream, nGenius, and nGeniusONE are registered trademarks or trademarks of NETSCOUT SYSTEMS, INC., and/or its subsidiaries and/or affiliates in the USA and/or other countries. Third-party trademarks mentioned are the property of their respective owners.

