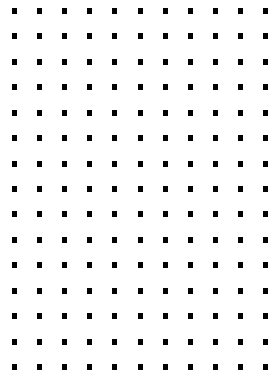


SOLUTION BRIEF

# Get Fast, Secure Wireless WAN for Your Industrial Edge



## Executive Summary

Digital transformation is creating greater efficiencies across the industrial sector. The Industrial Internet-of-Things (IIoT) has increased data capture for devices like sensors, gauges, and more. However, with these efficiency gains comes increased risk. And the stakes are even higher when the industrial equipment controls the critical infrastructure running cities, buildings, production lines, and the electric grid.

Gartner research shows that by 2025, cyberattackers will successfully weaponize industrial environments to successfully harm or kill humans.<sup>1</sup> Additionally, Gartner predicts that 75% of CEOs will be personally liable for cyber-physical security incidents.<sup>2</sup> This is an enormous burden, not only on the shoulders of industrial IT teams, but also their executive leadership.

Despite these challenges, the need to support digital innovations and serve today's market remains. How can your organization scale while remaining secure and operating without interruption? Read on.

According to a recent **State of Operational Technology and Cybersecurity Report** from Fortinet, over **90%** of organizations using some form of OT have a cybersecurity incident annually.<sup>3</sup>

## Extending the Reliability of Edge Broadband

FortiExtender is a secure wireless WAN gateway from Fortinet. FortiExtender cellular gateways add LTE/5G wireless connectivity to your industrial edge so you can securely support the latest digital innovations.

Connect your corporate, retail, and industrial sites regardless of wired broadband availability with FortiExtender. It is a cellular gateway that can extend and ensure the reliability of your edge broadband, while also securing local internet breakouts in a single pane of glass via the [Fortinet Security Fabric](#).

## Reliably Deploying LTE/5G at the Industrial Edge

Fortinet is the only wireless WAN vendor that can enable OT infrastructure teams to safely and reliably deploy LTE/5G at the industrial edge. Our FortiExtender cellular gateways and Secure SD-WAN solution are centrally managed alongside [FortiGate NGFW](#) on a single [FortiOS](#) operating system, creating the highest-performing cybersecurity mesh. As a result, all your policies and protections are unified.

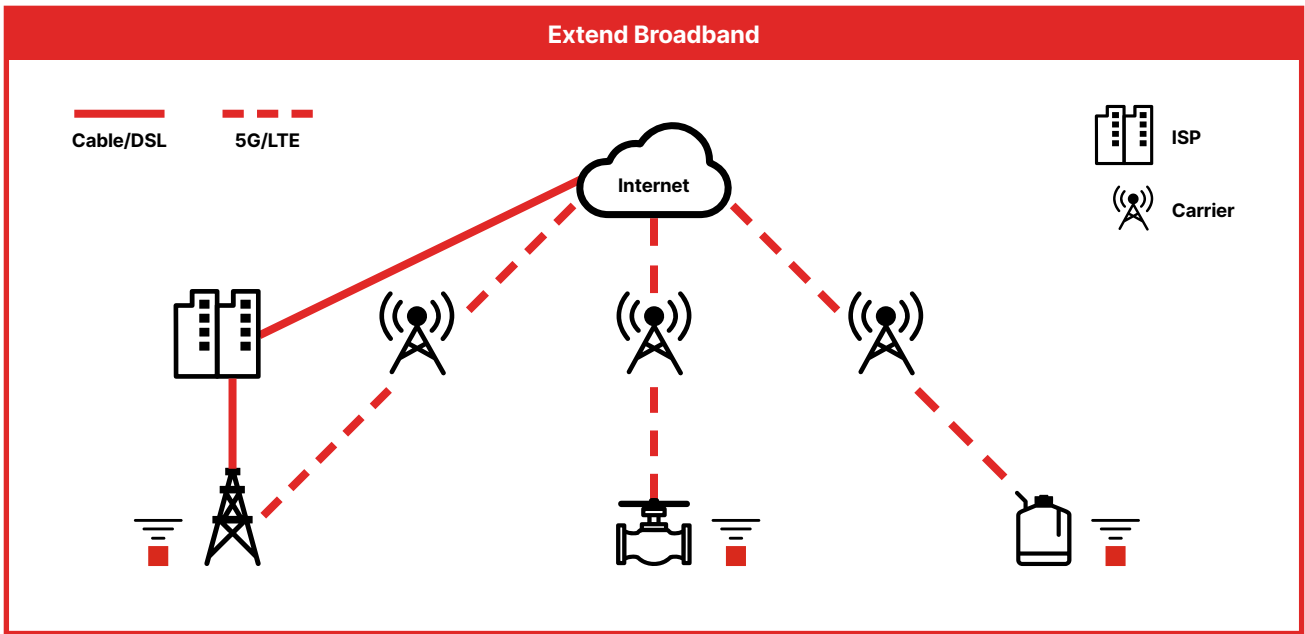
Connect, automate, and secure your corporate, retail, and operational sites with industry-leading network management and security. Fortinet has been named multiple times as a leader in the Gartner Magic Quadrants for WAN Edge Infrastructure and NGFW. We provide critical networking and security convergence that includes LTE/5G wireless WAN from FortiExtender.

## Adding Wireless WAN Links to OT Networks

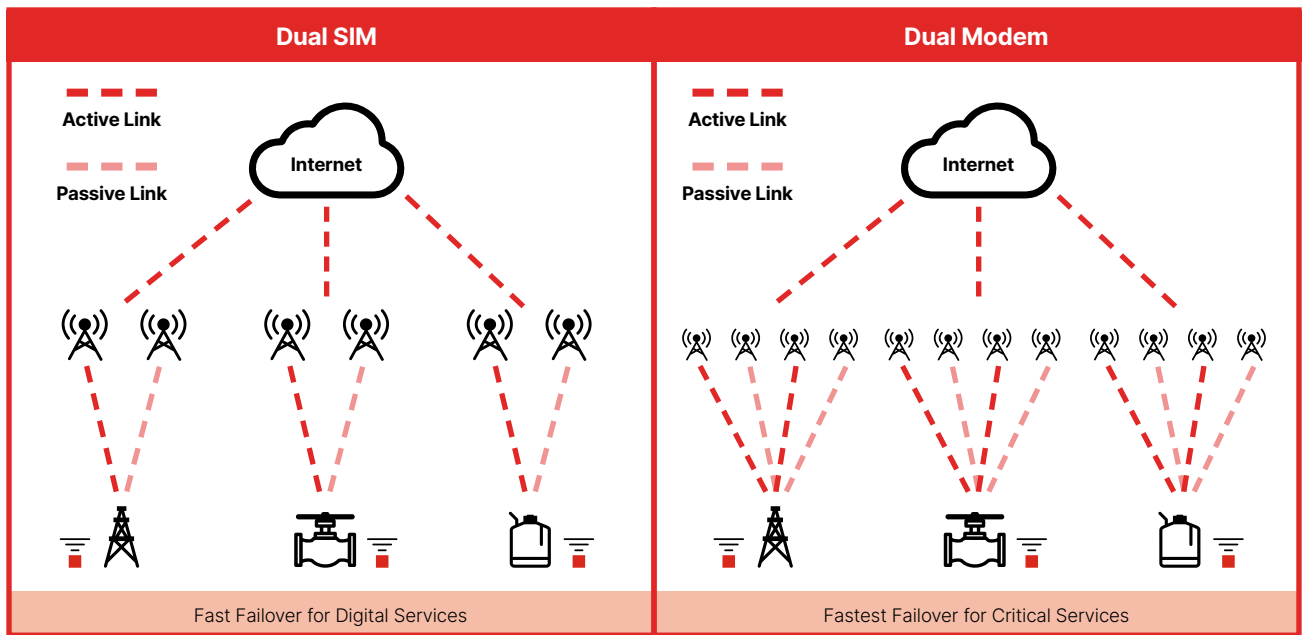
FortiExtender cellular gateways add gigabit-class and multigigabit wireless WAN links to your OT network. They are fully integrated in [Fortinet Secure SD-WAN](#) and enjoy the same NGFW protections over wireless connections. FortiExtender cellular gateways also provide:

- **Extended bandwidth:** FortiExtender cellular gateways can expand your connectivity to branches in locations that lack fixed broadband.





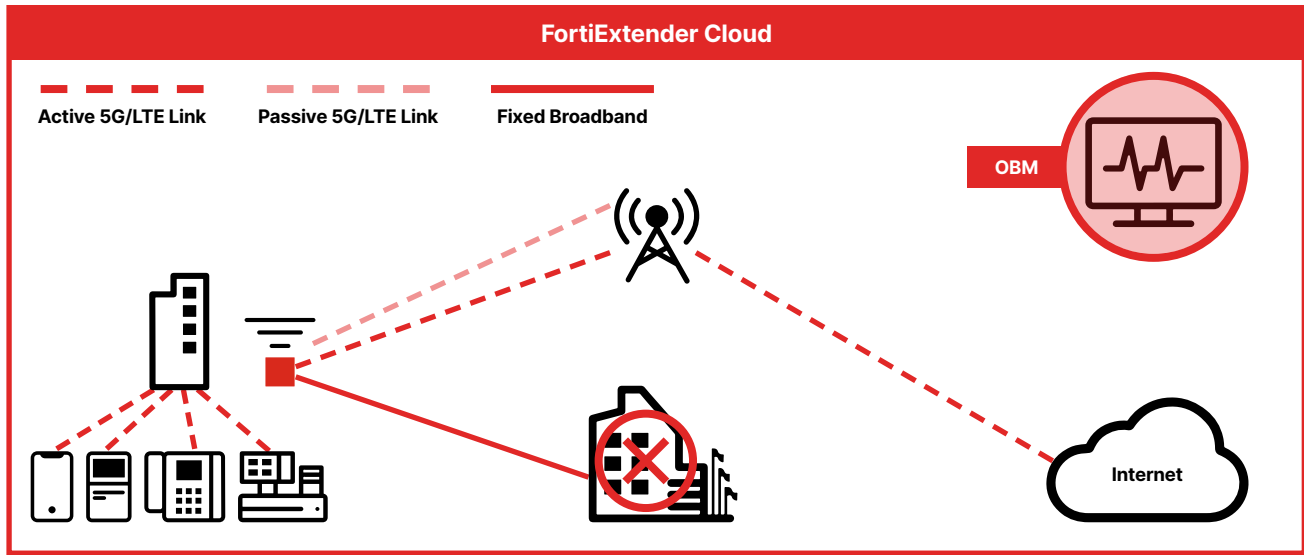
**Failover and high availability:** FortiExtender dual-SIM models contain two SIM card slots allowing for active/passive cellular links from separate ISPs. FortiExtender dual-modem models contain four SIM card slots, providing active/active links for high availability as well as load-balancing across cellular links.



**Out-of-band management (OBM):** FortiExtender cellular gateways provide critical business continuity capabilities through the FortiExtender Cloud dashboard. FortiExtender OBM allows enterprises to continue site device management outside of the traditional provider network and deliver consistent connectivity even in the event of a wired link disaster or outage.

Other solutions only provide OBM in specific and rare scenarios, such as a private IP network (closed APN), or with a public routable IP to the SIM card. These deployments are not typical. With FortiExtender, OBM works in any scenario.





**Integrated NGFW and Secure SD-WAN:** While opening OT locations to the internet can help cut network costs and increase convenience for the IT team, egress points on the network increase its attack surface and open the enterprise to security threats and all associated ramifications. FortiExtender cellular gateways enjoy the full spectrum of security controls from Fortinet at no extra cost.

Enjoy multilayered security to protect your operational consoles, connected devices, and people from the latest threats, thanks to integration with the Fortinet Security Fabric. In addition, integrated Secure SD-WAN gives you the power to automate QoE benchmarks on cellular links, specifying minimum criteria for loss, latency, and jitter. Bring up sites remotely through the FortiGate or FortiManager console—your FortiExtender cellular gateway appears as an additional interface in your network.

## Outcome Expectations

Oil and gas companies that use FortiExtender on their networks have enjoyed many benefits as a result. FortiExtender cellular gateways can:

- Increase a company's network reliability up to 4X
- Reduce a company's attack surface by 85%
- Expand a company's cloud access to 50% more locations

## Summary

FortiExtender cellular gateways greatly improve the security and reliability of your wireless WAN deployments. The gateways from Fortinet add gigabit-class and multigigabit cellular links that are fully automated, managed, and monitored in the FortiGate or FortiManager dashboard, and enjoy the full suite of NGFW protections thanks to their complete integration with the Fortinet Security Fabric.

<sup>1</sup> "Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans," Gartner Press Release, July 21, 2021.

<sup>2</sup> "Gartner Predicts 75% of CEOs Will be Personally Liable for Cyber-Physical Security Incidents by 2024," Gartner Press Release, September 1, 2020.

<sup>3</sup> "2021 The State of Operational Technology and Cybersecurity," Fortinet Report, 2021.