ERICSSON

Checklist: Fast-tracking secure IoT deployments

As organizations expand their IoT initiatives, connecting assets securely and reliably across dispersed sites is no longer optional; it's mission critical. Whether for smart kiosks, automation sensors, EV charging stations, or remote monitoring systems, this checklist offers a phased approach to help teams plan, deploy, and secure IoT devices on 5G networks, ensuring a fast, secure, and successful rollout.

Phase 1: Pre-deployment

Start with clear goals and a cross-functional team

- Have you defined the objectives and success metrics for this deployment?
- Is the IT team leading the deployment, or is a different group in charge?
- Do all stakeholders understand and agree on the use cases?

Lay the foundation for secure, scalable connectivity

- Do you understand the bandwidth and latency requirements for this deployment?
- Have you evaluated cellular coverage and data plans at each location?
- Have you mapped the end-to-end data flow for this deployment?
- How are you going to secure IoT data traffic across the cellular WAN?

Future-proof your solution

- Have you planned for scalability, upgrades, and increased traffic/load?
- How will you perform lifecycle management for IoT devices and the cellular routers?
- Have you modeled worst-case security scenarios and mitigation plans?

Phase 2: Deployment readiness

Equip your team for success

- Can routers accommodate future features such as network slicing and link bonding?
- How will you enable secure access to IoT devices for monitoring and maintenance?
- Do third parties need access?
- Are devices ruggedized and suited for extreme environmental conditions?
- Is there WAN redundancy (i.e., public/private cellular, wired, satellite) to ensure always-on connectivity?

Enabling intelligent, secure operations

- Are networks segmented to isolate critical systems?
- Have you considered zero trust vs. traditional VPN or private APN when connecting to private applications?
- Is out-of-band management available if remote infrastructure devices are lost?
- How will you monitor traffic for signs of malicious activity and enforce security policies?

Align IT and OT teams on lifecycle management

- Have you planned for centralized visibility and remote management, including cellular insights dashboards and live health stats?
- Are clientless and client-based ZTNA options available for remote employees and third-party vendors who need secure, role-based access?
- Is the solution AI-enabled to streamline support and detect performance anomalies?
- Has your team received training on device management, security, and installation?
- Do you need to run containers and SDKs on the edge?
- Does your management platform support deployment and orchestration at scale?

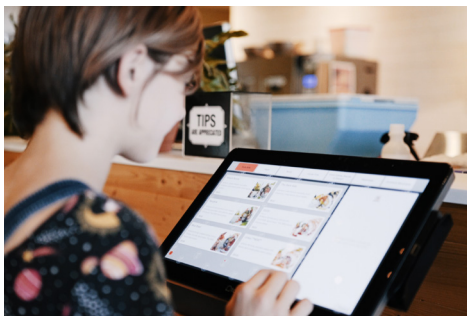

Image source: Getty Images

Quick check:

IoT cellular networking readiness scorecard

Use this quick check to see where you stand

Capability	Seeking solution	Solution in place
Ruggedized cellular routers		
Comprehensive centralized management		
Hybrid WAN connectivity with bonding and SD-WAN		
Location services for tracking assets		
ZTNA for secure remote access for internal and third parties		
Embedded zero trust to secure traffic to private data centers		
Out-of-band management capability		
AI-driven support and performance anomaly detection		
Application visibility and control		
SDK/Docker container support with simple orchestration		