Are Your Multi-Network IoT SIMs Secure?

A Practical Cybersecurity Checklist for IoT Deployments

When it comes to connecting IoT devices, multi-network SIM cards are a powerful tool. They keep devices online across carriers, regions, and borders—providing reliability in places where single-carrier coverage falls short. That flexibility, however, also introduces complexity. Every new connection path is another potential entry point for attackers.

For organizations that rely on IoT at scale, securing multi-network deployments is not optional—it's foundational. The good news is that most risks can be managed with the right configuration and oversight. The key is knowing which questions to ask about your setup.

This guide provides a cybersecurity checklist you can use to evaluate your current deployment, close gaps, and strengthen your defenses.

CHECKPOINT 01

Network Security: Controlling the Data Path

The first step in IoT security is ensuring that device traffic isn't needlessly exposed. Even if your carrier networks provide a layer of protection, you can't assume that coverage across multiple carriers is consistent.

Ask yourself:

- ☐ **Traffic Isolation:** Are IoT devices segmented from the public internet, using tools like private APNs, VPN tunnels, or firewalled static IPs?
- ☐ **Encryption:** Is every connection encrypted end-to-end with TLS 1.2 or stronger?
- ☐ **Policy Enforcement:** Can you restrict inbound and outbound traffic to only the IP addresses, services, or applications you trust?
- ☐ **Visibility:** Do you have centralized monitoring that can detect unusual usage or suspicious destinations, even as devices roam across different networks?

The goal: build a traffic environment where every packet is protected, and every anomaly is visible.

CHECKPOINT 02

Device Security: Hardening the Endpoint

A secure network doesn't mean much if endpoints are unprotected. IoT devices are often deployed in large numbers and in hard-to-reach places, which makes them prime targets if they're left with weak configurations.

Questions you should be asking include:

- ☐ **Unique Identity:** Are devices provisioned with unique credentials or certificates to ensure they can be individually identified and managed?
- ☐ **Configuration Hygiene:** Have default passwords and open ports been disabled before deployment?
- ☐ **Patch Readiness:** Can you push firmware updates and security patches remotely, quickly, and at scale?
- ☐ **Encryption:** Is any sensitive data stored locally on the device encrypted to prevent exposure if accessed?
- ☐ **Physical Security:** Is there tamper resistance or detection in place to prevent SIM swaps, device cloning, or unauthorized physical access?

Locking down devices before they're deployed—and keeping them updated throughout their lifecycle—eliminates many of the vulnerabilities attackers look for.

CHECKPOINT 03

Operational Practices: Managing Access and Response

Even strong network and device protections can fail without the right operational controls. IoT security isn't just a matter of technology; it's about who has access, how incidents are handled, and whether policies align with regulations.

Key questions:

- ☐ **Access Controls:** Who can activate, deactivate, or provision SIMs—and is that process logged and audited?
- ☐ **Incident Response:** If a device is compromised, can you suspend its connectivity immediately?
- ☐ **Compliance:** Are you aligned with standards like NIST, ISO 27001, or IEC 62443? Have you accounted for data residency rules if your devices roam across borders?
- ☐ **Third-Party Risk:** Do your carrier or MVNO partners provide visibility into how they handle authentication, traffic routing, and roaming sessions?

Good operational hygiene ensures that even when incidents happen, they're contained quickly without widespread disruption.

Why This Matters

The value of IoT lies in scale—hundreds or thousands of devices connected and working together. But at scale, small missteps have outsized consequences. A single device misconfigured, or a single SIM left unmanaged, can expose an entire deployment.

Consider this:

- A lack of encryption at the network handoff could expose sensitive telemetry.
- A default password left unchanged could provide attackers with instant access.
- A missing incident response plan could leave a compromised device active long enough to do real damage.

Addressing these risks proactively isn't just about avoiding breaches—it's about safeguarding uptime, protecting investments, and ensuring your IoT deployments deliver the outcomes they were designed for.

The Solve Networks Perspective

At Solve Networks, we've seen firsthand how connectivity can either strengthen or undermine IoT security. Multi-network SIMs unlock adaptability and resilience—but only when paired with the right controls. That's why we design connectivity solutions with reliability, visibility, adaptability, and security at their core.

- **Reliability:** Unsteered access across carriers ensures devices always find the strongest signal.
- **Visibility:** Real-time monitoring gives you insights into traffic flows and SIM health.
- **Adaptability:** Global eSIMs let you deploy once and adapt anywhere, without network lock-in.
- **Security:** Private static IPs, VPN support, and lifecycle management tools give you the guardrails you need.

Connectivity is the backbone of IoT, but security is what keeps that backbone from becoming a vulnerability.

Next Steps: Use the Checklist

Think of this checklist as a starting point. Even if you can answer "yes" to most questions, one or two "no" answers may highlight critical gaps worth fixing before your next deployment cycle.

Review your IoT security posture against this list. Share it with your IT and operations teams. Identify gaps and assign next steps.

Because when it comes to IoT, reliability without security is an illusion—and security without visibility is a gamble.