Challenge

Cellular Internet of Things (IoT) device applications are nearly unlimited; 5G will facilitate use even further.

However, concerns about security have slowed wide scale adoption of IoT devices. Vulnerable cellular networks experience denial-of-service attacks via fake cell towers, and hackers can easily collect data from any connected device from a point-of-sale to a commercial airliner.

Protect any connected device from network based attacks with FirstPoint's holistic cyber security protection

Comprehensive Protection for IoT Devices

FirstPoint provides carrier based protection and allows private networks to safeguard all connected devices while monitoring it all from a single dashboard.

Stop cyber-attacks before they happen by deterring attacks such as fake cell towers (aka IMSI catcher), cellular Man-in-the-Middle, and attacks that exploit emerging vulnerabilities impacting IoT devices. Our cybersecurity-as-a-service delivers total, easy to deploy, always on network-based security for every connected device.

FirstPoint covers the full spectrum of targeted and random cellular cyberattacks, including:

- ✓ SMS hijacking
- ✓ Location tracking
- ✓ Eavesdropping
- ✓ Local Denial-of-Service
- ✓ Remote Denial-of-Service
- ✓ Data leakage
- ✓ Data duplication
- ✓ Malware installation

Benefits for Enterprises

Simplify IoT adoption Increase trust; adapt for any use case; deploy in minutes

Obtain 360° protection
No more cellular network threats; no elements on carrier network; real-time visibility; always updated

Support any cellular device
Any cellular device; supports 2G-5G; via device or gateway, static or roaming, quick, infinite scaleup

Give users a hassle-free experience
No SW/HW, invisible to CPU

How it works

FirstPoint offers the following options, for implementation on a carrier or private network:

1. **Shared or dedicated server**: FirstPoint manages protected traffic at the MNO's data center, routing protected device traffic through either a shared or dedicated server.

2. **Full on-premise**: The organization manages protected traffic via a dedicated server, with a direct link between the organization and the MNO. There is no link to FirstPoint.

3. For **private cellular networks or private EPC**, the system is always set up on premise, with no direct link to any external public mobile network operator.
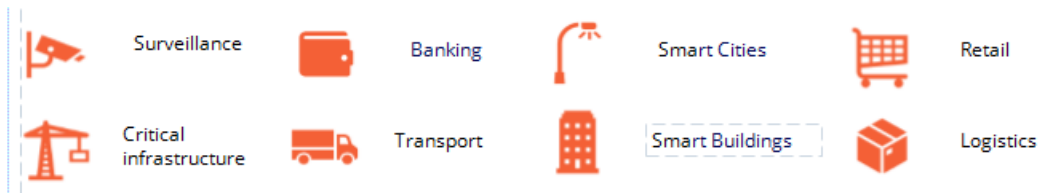
FirstPoint Secured
Virtual Network (SPLMN))

Simple, one-time, enterprise deployment

| 1 | Define the list of devices to protect (MSISDN/ IMSI) | 2 | SIM applet provided via Over-the-Air system or with new SIMs | 3 | Users operate devices as usual, manage at SOC |

IoT use cases: endless, but so are threats

IoT devices are used for an extensive number of applications. But that means more cellular cyber threats:

Surveillance   Banking   Smart Cities   Retail

Critical infrastructure   Transport   Smart Buildings   Logistics

FirstPoint knows how difficult it is to secure IoT devices from

cellular network cyberattacks.

We can help you protect any IoT device, anywhere

Talk to us about your needs, today: secure@firstpoint-mg.com

About FirstPoint

Israel-based FirstPoint protects any cellular device against hidden vulnerabilities in the network. Our agent-less, cellular network-based approach to cybersecurity identifies known and unknown attacks 24/7, instantly activating protective measures. FirstPoint solutions are completely transparent to the user/device, with no device installations, updates or slowdowns, protecting any device; e.g., mobile phones, M2M, security sensitive IoT and connected systems). Our team experts comprise cybersecurity and telecom veterans with decades of experience in interception, communications intelligence and cyber technologies.