Bridging Cellular and IT Security with Unified Context and Control

The Problem

As organizations adopt cellular connectivity across IT and OT environments, they face new security challenges. Cellular introduces unfamiliar attack vectors, diverse device types, and protocols that are not present in traditional networks. Maintaining full visibility and enforcing a Zero Trust posture becomes increasingly difficult as these environments expand. Devices often span multiple groups with unique security needs, yet IP-based management lacks the context required for accurate policy enforcement or effective remediation, creating complexity and greater exposure to threats.

Many OT networks also depend on non-cellular devices such as sensors, controllers, and gateways connected through cellular routers. Because only the router SIM is visible, these devices remain hidden, expanding the unmanaged attack surface. When threats arise, IP-based logs lack the device-level context needed to investigate and respond effectively.

Comprehensive, Context-Aware Security for Every Connected Device

Solution Benefits

- Device Fingerprinting: Identify every cellular and noncellular device.
- Unified Visibility: See all assets in one real-time view.
- Context Awareness: Detect SIM swaps, movement, and changes instantly.
- Adaptive Enforcement: Apply Zero Trust, context-based policies.
- Automated Protection: Block threats and streamline management.

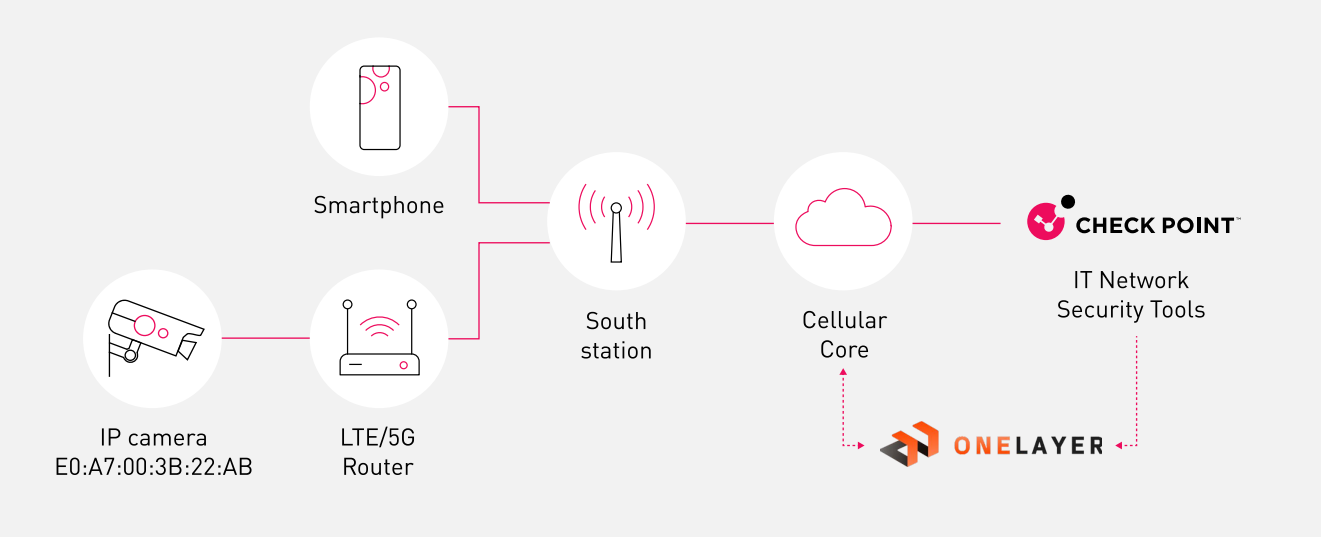
The Solution

Applying Zero Trust principles to cellular and noncellular devices is achievable through the integration of OneLayer Bridge and Check Point Network firewalls. OneLayer's proprietary fingerprinting technology provides continuous visibility and contextual intelligence for every connected device, correlating attributes like device type, manufacturer, SIM, and modem ID to establish a persistent identity.

This device context integrates seamlessly with Check Point SmartConsole, enabling adaptive, context-based policy enforcement. Check Point can automatically adjust policies as devices move, change IPs, or undergo SIM swaps, ensuring only authorized devices maintain access. The result is a unified, proactive approach that delivers consistent security across private and public cellular environments.

How It Works

The solution leverages OneLayer Bridge, which integrates with the Check Point, enriching Check Point Network firewalls with deep visibility into cellular network devices. Configured through the Check Point SmartConsole, the integration uses OneLayer's advanced fingerprinting to correlate device identity, behavior, and risk context for precise access control. This enables Check Point to enforce policies based on real, persistent device attributes rather than volatile identifiers like IPs or SIMs, ensuring continuous, device-aware protection across dynamic cellular environments.



The Check Point + OneLayer Advantage

The integration of OneLayer and Check Point brings together deep cellular visibility and advanced network enforcement to deliver Zero Trust security across every connected device.

BENEFITS	IMPACTS
Enhanced Visibility	Gain visibility and control of every connected device through unique fingerprinting, unified inventory, and real-time context awareness. Detect hidden assets, SIM swaps, and location changes to eliminate blind spots and strengthen Zero Trust security across all environments.
Stronger Security	Enforce real-time, context-based policies that adapt to each device's identity, behavior, and risk. Block unauthorized access, prevent lateral movement, and maintain Zero Trust protection across all connected environments.
Scalable Management	Automate policy updates and streamline operations with unified visibility and seamless integration across existing systems. Simplify management at scale while ensuring consistent control and responsiveness as devices, users, and networks evolve.

Use Case 1: Enforcing Device Whitelisting for Non-Cellular Assets

Challenge

In a modern manufacturing plant, systems such as robotic arms and controllers connect through cellular routers to reach operational networks. These routers can unintentionally permit unauthorized devices if not properly managed. While a MAC whitelist is maintained in the CMDB, static lists quickly become outdated, leaving traditional firewalls unable to verify device identities and exposing the network to rogue assets.

Solution

OneLayer integrates with Check Point to continuously validate devices connecting through cellular routers against the CMDB whitelist. Its fingerprinting technology identifies both cellular and non-cellular devices by key attributes and shares this context with Check Point for policy enforcement. Unauthorized devices are automatically blocked or quarantined.

Use Case 2: SIM Swap and Anomaly Detection

Challenge

Unauthorized SIM swaps can allow rogue devices to impersonate legitimate assets and access sensitive networks. When a SIM is moved to another device, traditional tools still recognize it as trusted, creating a blind spot attackers can exploit to bypass controls and move laterally within OT or enterprise environments.

Solution

OneLayer's SIM-swap detection continuously correlates SIM, IMEI, and device identifiers to verify each SIM's authorized hardware profile. When a mismatch occurs, OneLayer alerts Check Point to automatically block or quarantine the rogue device. This integrated response closes a critical visibility gap and prevents attackers from exploiting cellular access as an entry point.

Use Case 3: Context-Based Policy and Dynamic Segmentation

Challenge

Devices in manufacturing or logistics environments frequently change IPs or locations, making it difficult to maintain consistent policies.

Solution

OneLayer detects these property changes in real time and updates device context within Check Point's network groups. Check Point then applies the appropriate policy automatically, maintaining accurate segmentation and reducing manual intervention.

About Check Point

Check Point Software Technologies Ltd. is a global cyber security leader protecting more than 100,000 organizations worldwide. Its mission is to secure enterprises' AI transformation. With a prevention-first approach and an open ecosystem architecture, Check Point helps organizations block advanced threats, prioritize exposures, and automate security operations across complex digital environments. The unified architecture simplifies protection across hybrid networks, multi-cloud environments, digital workspaces, and AI systems. Structured around four strategic pillars, Hybrid Mesh Network Security, Workspace Security, Exposure Management, and AI Security, Check Point delivers consistent protection and visibility across multivendor environments, enabling organizations to reduce risk, improve efficiency, and accelerate innovation without increasing complexity.

ABOUT OneLayer

OneLayer transforms enterprise cellular environments from operational silos into integrated networks, embedding cybersecurity, observability, and orchestration into every private cellular deployment. The OneLayer Bridge platform secures and manages both private 5G/LTE networks and private APNs running over public cellular infrastructure, providing unified visibility and consistent policy enforcement across IT and OT ecosystems.