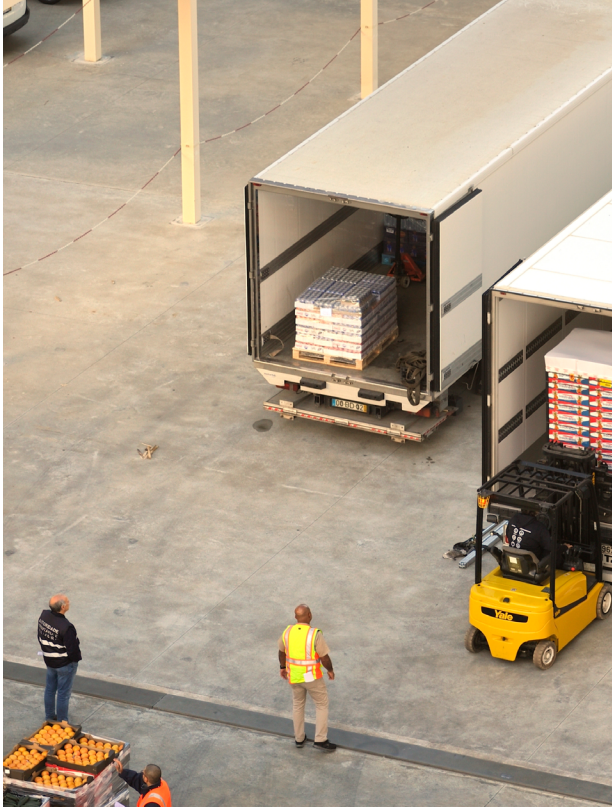


ENFORCEMENT SERVICE BRIEF

Aeris IoT Watchtower™



OVERVIEW

IoT connected devices are extremely hard to protect from external hackers or hidden backdoors due to their diversity, resource constraints, lack of standardization, and limited update mechanisms. These factors, combined with weak authentication, network exposure, and supply chain vulnerabilities, necessitate a robust cellular specific solution like Aeris IoT Watchtower for comprehensive security. Aeris IoT Watchtower is the world's first and best security solution to provide visibility into cellular IoT security threats. Watchtower proactively blocks or mitigates security incidents and provides material risk reduction and regulatory compliance for cellular based IoT deployments.

IOT CHALLENGES AND WHY AERIS IOT WATCHTOWER

01 The risk and cost of a cybersecurity incident related to an IoT deployment can be astronomical. Devices stay in the field for a long time, and and may not be patched remotely or replaced economically. OTA upgrades can be risky. Aeris IoT Watchtower materially reduces that risk. Watchtower enables you to avoid business catastrophes such as downtime, revenue loss, penalties, or brand damage.

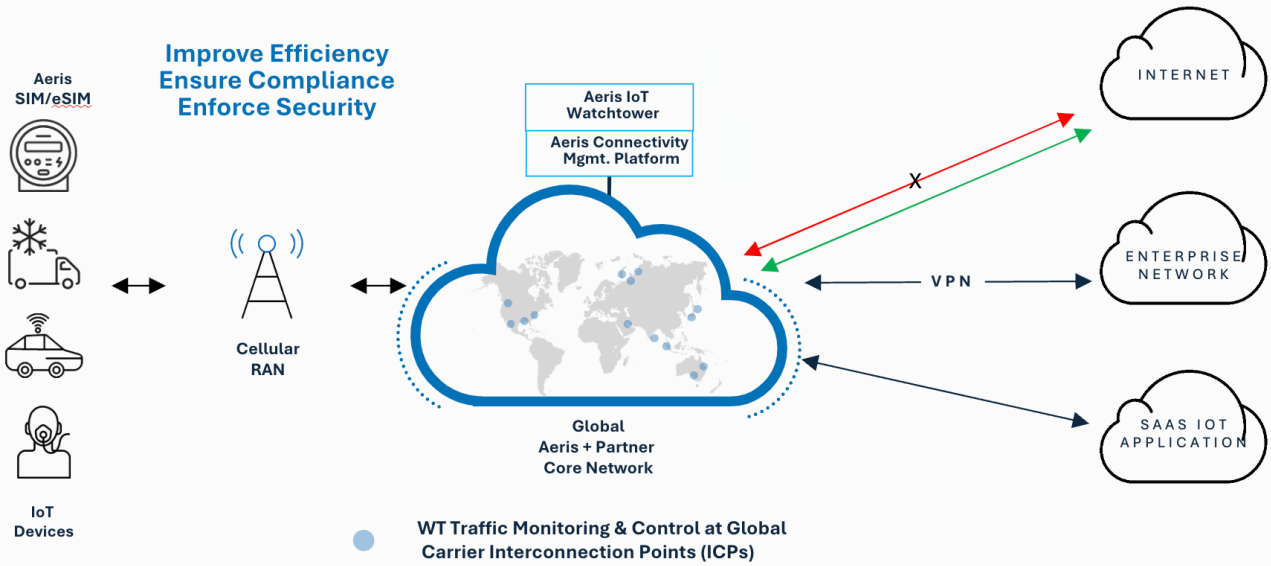
02 IoT devices are very hard to secure, as they are physically remote and quite often do not have an individual user associated with them. In addition, they have limited processing and software capability to support security solutions traditionally aimed at laptops. Aeris IoT Watchtower solves this issue with an agentless, network-based solution.

03 It is very difficult for an Enterprise to know all of the (supply chain) software bill of material in an IoT device, and many IoT devices have backdoors built into them for the hardware supplier or radio module supplier. Aeris IoT Watchtower solves the lack of insight into backdoors by seeing all traffic and alerting if traffic is going to a destination outside of the designed purpose of the device.

04 Nation state-based attacks and the related critical infrastructure cyber regulation is growing, and fines are increasing for non-compliance. Aeris IoT Watchtower provides both protection and auditable documentation for compliance with regulations.

HOW IT WORKS

Aeris IoT Watchtower leverages the native instrumentation and control mechanisms of the cellular packet core data network, offering customers a streamlined solution that maintains global, uniform security policies and connectivity management. Everything is done at the network level, there is no impact to your network, applications, or devices. No agents. No trust brokers. No additional hardware to deploy. Partners leverage the Aeris Core Network to extend their existing connectivity services, without replacement or disruption.



Aeris IoT Watchtower leverages a real time database of IoT device, application, and server communications. Watchtower leverages AI/ML to alert on security issues and compares the data to known threat databases. In addition to awareness of the issue, Watchtower provides capabilities to mitigate by quarantining events, blocking devices, or preventing threats through zero trust policies.

From the Management Platform, you have access to real-time and historical device behavior. It enables you to visualize trends, handle events, create Zero Trust application access policies, run reports, manage, and scale your global IoT deployments.

BUSINESS VALUE

Aeris IoT Watchtower delivers substantial business value across three key dimensions: It helps improve operational efficiency, ensure that organizations meet their compliance obligation and provide visibility to enable policies that enforce security.

AWARENESS

01

FEATURE

- Monthly security assessment report
- Continuous monitoring into indicators of compromise
- Agentless
- Asset inventory of cellular devices and traffic metering
- Real time per device insights and deep diagnostics

02

VALUE

- Auditable documentation for proof of regulatory compliance
- Quickly identify and respond to compromised or defective devices
- Support all device types, for existing and new installations
- Simplify inventory management
- Avoid spurious traffic spikes draining resources
- Faster timeto redsolution

ENFORCEMENT

01

FEATURE

- Set and enforce policy
- Self-service response
- Limit device access to explicitly authorized destinations

02

VALUE

- Enforce policy control on all device types
- Enforce policy without affecting the device operations
- Prevent exploitation of known vulnerabilities
- Minimize the attack surface

COMMON MISCONCEPTIONS

Many organizations believe their current security solutions suffice.

My Corp IT security is sufficient: Securing corporate infrastructure solutions are very different from securing cellular-connected devices which are scattered globally, lack a user, a standard operating system and limited security tools mitigating the risk to the device. Traditional solutions and NAC policies lack visibility into cellular devices without an agent, making it difficult to identify compromised devices. If an IoT device is compromised, it can be the interpoint throughout the corporate network, enabling lateral movement. Additionally, local Internet breakouts can bypass corporate security measures, leaving data traffic exposed and vulnerable. Ensuring robust protection for these devices is crucial to preventing security gaps.

Aeris owns the core network and Aeris IoT Watchtower is in line with the data traffic preventing it from being bypassed.

Encryption, VPNs and Private APNs are sufficient: Another common misconception is that encryption, VPNs, and private APNs are sufficient for security. However, these devices—whether they are smart meters, fleet tracking systems, or connected cars—are spread worldwide and often have vulnerabilities like outdated or open-source software. These protections cannot detect or block unexpected traffic from compromised devices trying to reach unauthorized destinations. Once a device is infected due to its inherent vulnerabilities, it can potentially go anywhere and pose significant security risks.

Aeris IoT Watchtower provides additional protection to existing security mechanisms like encryption, VPNs and Private APN to detect and prevent unexpected traffic from compromised devices going to unauthorized destinations.

Aeris IoT Watchtower provides a layered approach to existing security mechanisms through visibility and enforcement for cellular IoT making Aeris IoT Watchtower the best solution.

Firewall service is sufficient: Firewalls (FW) are essential for IT security, offering crucial protection by monitoring network traffic. However, they often lack granular visibility into individual IoT devices and struggle with comprehensive threat intelligence and scalability. Aeris IoT Watchtower complements firewalls by providing per-device monitoring, advanced threat intelligence with coverage of Indicators of Compromise (IoC), and the ability to create specific policy groups.Aeris IoT Watchtower's self-service platform simplifies management, offering cost-effective, efficient solutions that outperform traditional firewalls, especially in complex IoT environments. Integrating Aeris IoT Watchtower with your firewall services ensures enhanced visibility, comprehensive protection, and operational efficiency across both IT and OT spaces, delivering a robust, scalable security solution

REGULATIONS, FRAMEWORKS AND STANDARDS

The rapid expansion of IoT has increased focus on securing devices against cyber threats. All industries face regulations and penalties. IoT regulations have matured, focusing on three primary objectives:

- Enhancing IoT cyber security to make connected devices more resilient against cyber threats
- Safeguarding the infrastructure and
- Enabling personal information privacy within IoT

ALL VERTICALS

- EU Cyber Resilience Act
- NIS2 Directive
- Product Security and Telecoms Infrastructure Act (PSTI) (U.K.)
- ETSI EN 303 645 and TS 103 645
- SEC Cyber Disclosure FRule (U.S)
- IEC 62433 Automation and Control Cybersecurity Standards

ENERGY AND UTILITIES

- IEC 62351
- NIST SP 1108
- NERC-CIP

AUTOMOTIVE

- UNECE WP.29 R155
- ISO/SAE 21434
- PAS 1885

Different regulatory frameworks and other regulations govern various aspects of IoT deployments, from data security to infrastructure and business operations. Aeris IoT Watchtower is positioned to provide visibility and enforcement for IoT threats on a granular per device level in addition to creating audit documentation to provide proof of compliance.



© 2025 Aeris Communications, Inc. All rights reserved. Aeris® and its logos, as well as other referenced marks, including Aeris IoT Watchtower™ and Aeris IoT Acuity™ are trademarks or registered trademarks of Aeris Communications, Inc. and its subsidiaries or affiliates. No portions or content of this document may be displayed or reproduced without prior written consent of Aeris Communications, Inc. Specifications are subject to change without notice.

CONTACT YOUR LOCAL SALES REPRESENTATIVE TO LEARN MORE