

---

# Reducing Costs in IoT

How to assess and reduce  
Total Cost of Ownership in IoT

---

# Why Business Leaders should **Prioritise Total Cost of Ownership (TCO)** in IoT Projects

The Internet of Things (IoT) has transformed industries by enabling smarter operations, enhanced customer experiences, and new business models. However, the complexity and scale of IoT deployments demand rigorous financial planning, making Total Cost of Ownership (TCO) a critical metric. Prioritising TCO allows business leaders to assess the long-term value and sustainability of IoT initiatives, ensuring strategic alignment and cost efficiency.

## 1. Long-Term Financial Predictability

IoT projects often involve high initial investments in devices, infrastructure, and software, alongside ongoing operational costs. A focus on TCO enables leaders to avoid cost overruns and allocate resources effectively and foster fiscal discipline.

## 2. Risk Mitigation

TCO analysis helps identify hidden costs, such as maintenance, upgrades, and cybersecurity measures. For example, IoT devices can be prone to vulnerabilities that can result in significant expenses from breaches.

## 3. Operational Efficiency

IoT systems integrate devices, networks, and data platforms, often across global supply chains. TCO analysis highlights areas where optimisation—like SKU rationalisation or remote device management—can reduce costs.

## 4. Enhanced Scalability

IoT deployments frequently evolve in scope as businesses expand or adopt new use cases. Understanding TCO ensures that solutions are scalable without exponentially increasing costs. Leaders can evaluate the trade-offs between initial investments and long-term benefits, ensuring that infrastructure and platform choices support growth while maintaining cost-effectiveness.

## 5. Improved Stakeholder Confidence

Investors and stakeholders prioritise transparency and accountability in major initiatives. A detailed TCO framework demonstrates that leaders have thoroughly evaluated the financial viability of IoT projects. This enhances trust and positions the organisation as a disciplined and strategic innovator.

## 6. Competitive Advantage

Businesses that control IoT costs effectively can reinvest savings into innovation, customer engagement, or market expansion. For example, reducing the lifecycle costs of devices allows companies to price competitively or offer enhanced services, boosting market share and brand loyalty.

## Conclusion

By prioritising TCO in IoT projects, business leaders can ensure financial prudence, operational resilience, and strategic success. This holistic approach transforms IoT from a technological ambition into a sustainable business asset, enabling organisations to thrive in a competitive and dynamic landscape.

# Contents

<b>A 12-point framework for managing TCO – the known and the unknown</b>	<b>4</b>
<i>Major sources of cost in IoT?</i>	4
<i>What about the unknown?</i>	5
<b>TCO Dashboard: Key cost considerations and how to manage them</b>	<b>8</b>
<b>Hidden costs of cutting corners</b>	<b>10</b>
<i>Myth Busting – Cellular is expensive for IoT</i>	10
<i>SKU Proliferation</i>	11
<i>Device Recalls</i>	13
<i>Cyber-security Breaches</i>	14
<i>Outages and Recovery</i>	15
<b>Advanced Network, SIM and Service capabilities which will help you reduce TCO</b>	<b>16</b>
<i>Myth Busting – Low power doesn't always mean low cost</i>	18
<i>Create a single SKU with eSIM &amp; iSIM</i>	20
<i>Remote SIM Provisioning</i>	21
<i>Device Management</i>	22
<i>Application Enablement Platforms (AEPs) with Low-Code Development</i>	23
<i>End-end Solutions</i>	24
<i>Fully Managed Services</i>	25
<i>IoT Security Framework</i>	26
<i>Global 24/7 Operations</i>	27
<b>Contact Wireless Logic</b>	<b>28</b>

IoT services and connectivity are not a commodity to be added at the last minute or left for the end-user to configure.

Building it into devices and applications from the start delivers resilience, security, and the agility to adapt to changing commercial, regulatory, and cross-border market conditions.

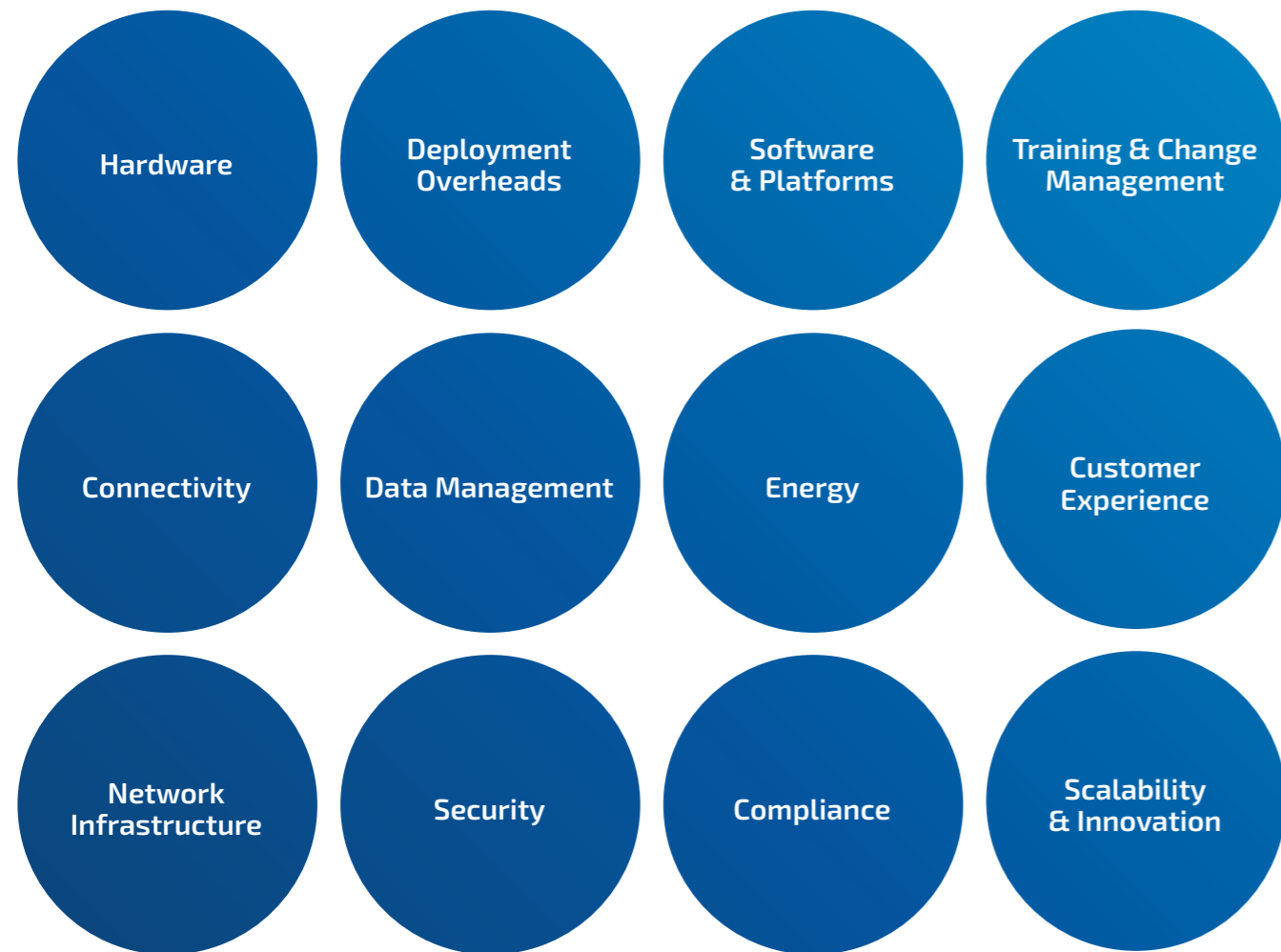
# A 12-point framework for managing TCO

## – the known and the unknown

The IoT landscape continues to evolve and grow at pace. As ever, managing Total Cost of Ownership (TCO) is critical for long-term success. Without a structured approach, costs can spiral due to overlooked factors like infrastructure, maintenance, or security risks.

This paper presents a 12-point TCO framework which provides a systematic way to evaluate and control these costs, ensuring that IoT deployments remain cost-effective, scalable, and resilient. It covers the 12 well-understood areas listed below but it is also vital to anticipate and address the unknown

### Major sources of cost in IoT?



### What about the unknown?

Unknown costs—such as those arising from outages, security breaches, or regulatory compliance—can disrupt IoT projects and inflate budgets. A proactive approach is essential: robust planning, risk assessment, and implementing scalable, secure, and resilient devices and systems can mitigate these risks.

Leveraging frameworks and experienced partners helps anticipate challenges like compliance in new markets or evolving cyber threats. While unknowns can't always be eliminated, strategic foresight and adaptable solutions ensure businesses are prepared to handle them effectively, minimizing impact on TCO. These unknown or **Hidden Costs** will be covered later.



### Learn more...

...about how to maximise uptime and design for high-availability and cyber-resilience.

The cost of ownership in IoT (Internet of Things) deployments includes several factors that start with the initial purchase of devices but go well beyond.

These costs arise throughout the lifecycle of the IoT system and can be grouped into the following categories:

<b>Hardware</b>	Devices and Sensors: The initial cost of IoT devices, sensors, and actuators.
	Gateways: Cost of edge devices or gateways to aggregate and process data locally.
	Replacement and Upgrades: Cost for periodic replacement or upgrading of devices due to wear and tear, obsolescence, or new requirements.
<b>Connectivity</b>	Network Infrastructure: Setting up WiFi, LoRaWAN, cellular, or other communication networks.
	Bandwidth and Data Plans: Ongoing cost of data transmission, especially in cellular or satellite IoT deployments. <i>See <a href="#">Myth Busting – Cellular is expensive for IoT</a></i>
<b>Network Infrastructure</b>	Keep in mind that existing carrier networks (e.g., cellular, satellite) are operated and maintained by the service providers.
	Assess planning, installation and commissioning costs associated with private networks (e.g. WiFi, LoRaWAN). Factor in the long-term maintenance, security and scalability of private network infrastructure.
<b>Deployment Overheads</b>	Installation Costs: Deploying devices, gateways, and infrastructure requires labour, tools, and time, adding to initial expenses.
	Integration Complexity: Ensuring seamless compatibility with existing systems increases effort and costs.
	Geographical Challenges: Deployments in remote or diverse locations incur higher logistics and resource expenses.
<b>Data Management</b>	Storage Costs: Growing IoT data volumes require scalable and often costly storage solutions.
	Processing and Analytics: Real-time insights demand advanced processing capabilities, increasing operational expenses.
	Data Lifecycle Management: Implementation of secure data frameworks (including archiving, retention and deletion policies) add complexity and costs
	Accessing and sharing data will be essential for many businesses and industries. This adds complexity and costs.
<b>Security</b>	Upfront Investment: Minimise your costs by working with partners to implement robust encryption, secure boot, and threat detection systems.
	Ongoing Maintenance: Regular updates, patches, and monitoring to address emerging threats add to operational expenses.
	Incident Mitigation: Inadequate or slow response to breaches or vulnerabilities can incur significant recovery and reputational costs.

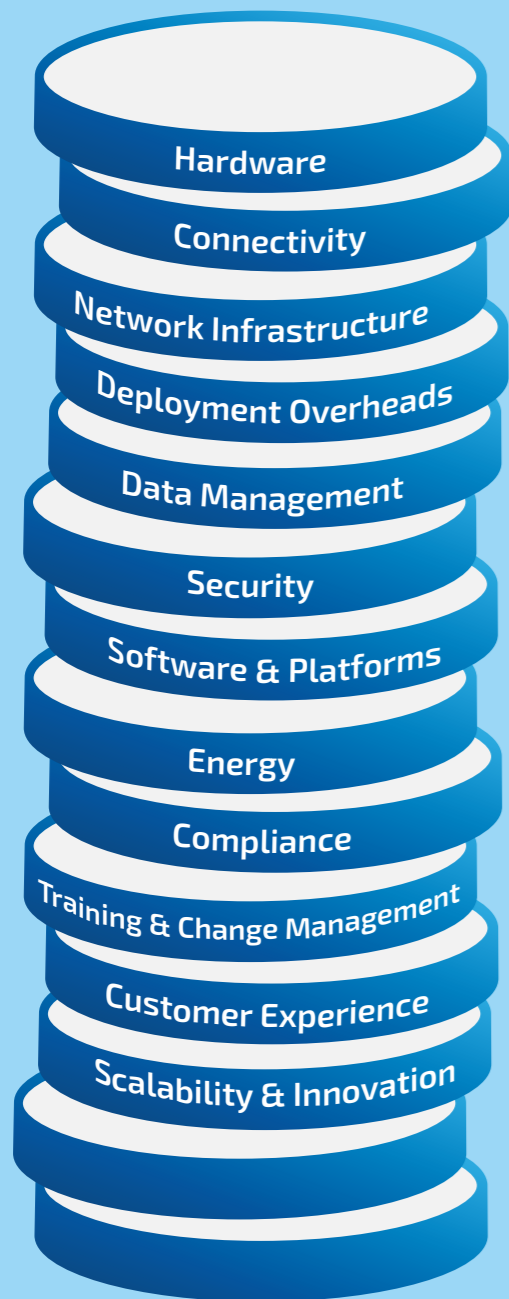
<b>Software &amp; Platforms</b>	IoT Platform Subscription: Costs for IoT platforms for device management, analytics, and application development.
	Licensing Fees: For proprietary software used in IoT applications.
	Custom Development: Costs for creating bespoke software solutions.
<b>Energy</b>	Power Consumption: Operational energy costs for devices, gateways, and network infrastructure.
	Battery Swaps or recharging: Design and technology choices can help extend battery life but might be offset by higher costs in other areas. <i>See <a href="#">Myth Busting – Low Power doesn't always mean low cost</a></i>
<b>Compliance</b>	Adapting to Regulations: Meeting diverse regional compliance standards increases design, testing, and certification costs, e.g. cellular roaming restrictions, cyber-security
	Ongoing Monitoring: Ensuring continued compliance requires monitoring, regular audits and updates, adding to operational expenses. Penalties and Redesigns: Non-compliance risks fines, legal actions, and costly product modifications.
<b>Training &amp; Change Management</b>	Employee Training: Upskilling staff on IoT systems incurs costs for materials, sessions, and lost productivity during training.
	Adoption Challenges: Resistance to change can slow implementation, leading to delays and increased expenses.
	Ongoing Support: Continuous updates and retraining add to long-term operational costs.
<b>Customer Experience (CX)</b>	Higher Support Costs: Poor CX leads to more complaints, increasing support and maintenance expenses.
	Lost Revenue: Bad CX drives customer churn, raising acquisition costs to replace lost users. Reputational Damage: Negative CX harms brand reputation, requiring extra investment in recovery and trust-building efforts.

By systematically evaluating these factors, organisations can identify their major cost drivers early and develop proactive strategies to mitigate them. This holistic approach prevents unexpected expenses and aligns technology choices with business objectives.

There could be numerous other business or application specific considerations in addition to those listed (decommissioning, disposal, recycling for example) so it's important that this TCO framework is not just used as a checklist. Consider it a starting point for developing a roadmap to sustainable IoT success, helping you stay competitive while optimising costs at every stage of your deployment.

# TCO Dashboard: Key Cost Considerations and how to manage them

## 12 point TCO framework



## Hidden Costs\* of Cutting Corners and how to avoid them

- Myth Busting**  
 Cellular is **expensive** for IoT
- SKU Proliferation** increases inventory carrying costs  
**~20–30% annually** [NetSuite]
- Truck Roll** can cost more than **\$1000 per site visit** [Sightcall]
- Device Recall** costs often **exceed \$10M** [Insurance Edge]
- Ransomware attacks** on IoT devices can cost **in excess of \$5M** [PurpleSec]
- Unplanned industrial system outages** cost businesses **\$100K per hour** [ABB]

\* Costs are proportional to company size and operational footprint

## Capabilities to demand from your IoT Service Provider which will help you reduce TCO

- Myth Busting**  
 Low Power doesn't always mean low cost
- Create a single SKU with eSIM & iSIM**
- Remote SIM Provisioning**
- Device Management**
- Application Enablement Platforms (AEPs) with Low-Code Development**
- End-end Solutions**
- Fully Managed Services**
- IoT Security Framework**
- Global 24/7 Operations**

# Hidden costs of cutting corners

## Myth Busting – Cellular is expensive for IoT

**Opinions around cellular connectivity (also Satellite) being expensive for IoT have evolved over time shaped by experience but also by the growing need for reliability and security.**

With cellular, the total cost of ownership (TCO) is often more favourable than with WiFi, Bluetooth, LoRaWAN, or Zigbee, especially when those networks are managed by 3rd parties with no stake holding in the IoT solution.

### Lower Infrastructure Costs

Cellular networks are deployed, maintained, and managed by Communication Service Providers (CSPs), eliminating infrastructure costs for enterprises. Businesses simply pay for data plans, with no need to install and maintain base stations or backhaul connections.

Alternatives like WiFi, LoRaWAN, and Zigbee require significant investment in gateways, access points, or mesh networks, especially if public or Enterprise infrastructure are unavailable. When they are, (in the WiFi case) they will rarely be optimised for IoT, leading to poor performance, increased maintenance, and degraded customer experience (CX). For example, 3rd party IoT devices (not on an approved IT or CISO list) may be blocked from Enterprise networks or over-looked during maintenance.

### Maintenance and Service Quality

Cellular networks are designed and managed with reliability, resilience, security and scalability as priorities. You must not assume that the same is always true in WiFi networks and should assess whether IoT-specific configurations and maintenance plans are in place. Issues with overloaded or poorly maintained networks result in higher repair costs, loss of service, and reduced CX.

### Security Risks

Cellular offers robust security with SIM-based authentication and encryption, minimising vulnerabilities. In contrast, domestic or commercial WiFi networks are prone to breaches, often requiring expensive mitigation measures. Poor security increases operational risks and raises TCO significantly.

In summary, **Cellular IoT provides 4 key benefits** and far from being costly, is often the smartest, most cost-efficient choice for IoT deployments.



**No infrastructure overheads:**  
*CSPs handle infrastructure*

**Reliability:**  
*Professionally managed networks maximise uptime*

**Scalability:**  
*Seamlessly supports large-scale deployments*

**Security:**  
*Enhanced protocols minimise risks*

## SKU Proliferation

**SKU Proliferation - creating multiple stock-keeping units (SKUs) to meet regional, functional, or customer-specific requirements - can significantly increase IoT deployment costs.**

In cellular IoT the SIM is an important consideration which if overlooked can undermine other hardware, software decisions made at the device design stage

Managing diverse SKUs results in higher production complexity, inventory management challenges, and increased overhead for logistics and compliance. This fragmentation also complicates testing, certification, and support processes, inflating the total cost of ownership (TCO) for IoT projects.

SKU proliferation increases inventory carrying costs  
**~20–30% annually**  
[NetSuite]



To address these challenges, businesses can adopt SKU rationalisation strategies:

### 1. Modular Design

By creating modular hardware and software components (including remote SIM provisioning) businesses can assemble products that meet diverse needs without maintaining separate SKUs. This approach reduces manufacturing complexity and improves scalability.

### 2. Global Certification

Investing in globally certified hardware and connectivity services eliminates the need for region-specific SKUs. A single SKU, including the SIM, can be deployed across multiple geographies, reducing compliance costs and simplifying logistics.



### 3. Software-Based Customisation

Shifting functionality from hardware to software allows businesses to use one hardware SKU with region- or customer-specific software updates. This approach minimises hardware variations while maximising flexibility. eSIM and iSIM-based solutions support this strategy.

By adopting these strategies, businesses can achieve significant cost reductions while simplifying operations, improving time-to-market, and maintaining flexibility in IoT deployments. Effective SKU rationalisation is key to optimising IoT TCO and ensuring long-term scalability.

For cellular connected devices, careful consideration of network availability, especially when it comes to NB-IoT, and LTE-M. Unlike LTE Cat-1, those technologies have not been implemented in all countries not by all carriers globally. The same care is also required for the SIM. SKU rationalisation at a SIM level is only achievable when working with service providers who can deliver flexible, future-proof solutions (see [Create a secure, single SKU with eSIM & iSIM](#)) which enable you to navigate the evolving commercial and regulatory compliance demands in different parts of the world.

## Hidden Costs of Cutting Corners *(continued)*

### Truck Roll

Truck Rolls—the deployment of field technicians to install, maintain, or repair IoT devices—are a significant cost driver in IoT deployments. Each truck roll incurs expenses for labour, fuel, vehicle wear, and often missed productivity opportunities.

For enterprises managing large or geographically dispersed IoT deployments, these costs can quickly escalate. Additionally, delays caused by the need for physical intervention can lead to extended service outages, further impacting customer satisfaction and operational efficiency.

Truck Roll can cost **more than \$1000 per site visit** [Sightcall]



To mitigate these costs, businesses can adopt the following avoidance strategies:

#### 1. Remote Monitoring and Management

Leveraging IoT platforms that support remote diagnostics and firmware updates reduces the need for physical interventions. Devices can be monitored and maintained from a centralised location, addressing many issues without deploying a technician.

#### 2. Predictive Maintenance

Implementing AI-driven analytics to predict potential failures enables proactive interventions before issues escalate. This minimises urgent, unplanned truck rolls and extends the lifecycle of devices.

#### 3. Modular Design and Easy Access

Designing devices with modular components or self-serviceable parts simplifies field maintenance, reducing the duration and frequency of on-site visits.

By adopting these strategies, enterprises can significantly lower operational costs, improve service efficiency and enhance the scalability of their IoT deployments.

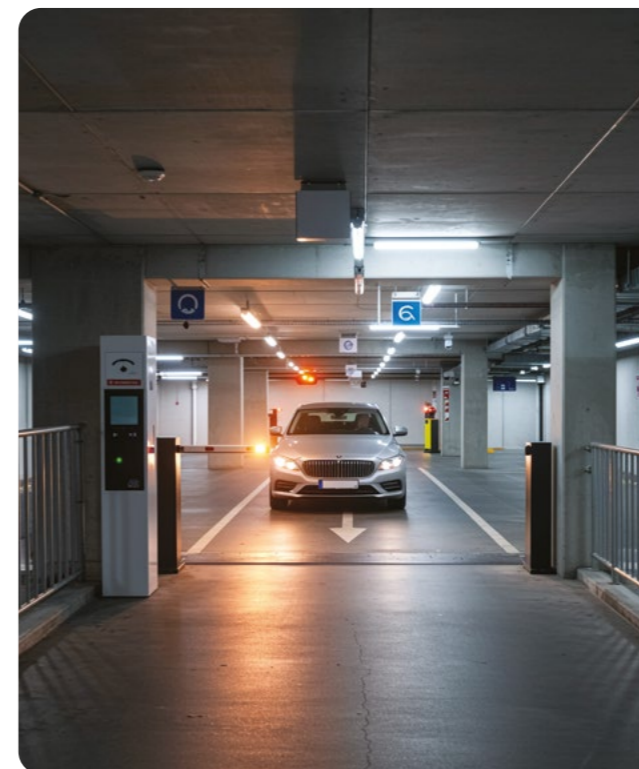
### Device Recalls

**Device recalls are among the most disruptive and costly challenges in IoT deployments.**

A recall can arise from hardware defects, software vulnerabilities, security breaches or non-compliance with regulatory standards.

These incidents lead to direct costs such as shipping, repairs, or replacements, and indirect costs like loss of customer trust, legal liabilities, and reputational damage. For large-scale IoT deployments, recalls can escalate exponentially due to the sheer volume of devices involved and the logistics required to recover or replace them.

Device Recall **costs often exceed \$10M** [Insurance Edge]



To mitigate recall risks, businesses can adopt these avoidance strategies:

#### 1. Rigorous Testing, Simulation and Quality Assurance

Thorough pre-deployment testing ensures devices meet performance and compliance standards. Using digital twins to simulate real-world conditions minimises the risk of undetected flaws.

#### 2. Over-the-Air (OTA) Updates

IoT devices equipped with OTA update capabilities can receive software fixes and security patches remotely. This eliminates the need for physical recalls for many issues.

#### 3. Proactive Monitoring and Analytics

Real-time device performance monitoring helps identify and address emerging issues before widespread failures occur, minimising the scope of potential recalls.

These strategies can be implemented using Device, Application and Security Management platforms to monitor everything from device temperature to full digital twins and device-cloud communication patterns. Doing so enables enterprises to significantly reduce the likelihood and impact of recalls, preserving customer trust and optimising IoT deployment costs.

## Hidden Costs of Cutting Corners *(continued)*

### Cyber-Security Breaches

Cyber-Security breaches are a critical risk for IoT deployments, often resulting in significant financial and reputational damage. Direct costs include incident response, forensic investigations, system downtime, and legal penalties, while indirect costs stem from loss of customer trust, compliance violations, and long-term reputational harm.

In large-scale IoT deployments, the interconnected nature of devices amplifies vulnerabilities, potentially allowing breaches to compromise entire networks or critical systems.

#### Ransomware attacks on IoT devices can cost in excess of \$5M

Prolonged breach will add significant financial burdens.

[PurpleSec]



To minimise these risks, businesses can adopt the following cybersecurity strategies:

#### 1. Secure Device Design

Building security into IoT devices from the outset reduces the likelihood of breaches. This includes secure boot mechanisms, encryption, and hardware-based authentication.

In the banking, payments and Enterprise IT domains authentication methods such as biometrics, digital certificates or multi-factor authentication are now standard. IoT SAFE (a GSMA standard) enables these strategies to be implemented cost-effectively in IoT devices.

#### 2. Regular Security Updates

Implementing firmware-over-the-air (FOTA or OTA) updates ensures that devices remain protected against emerging threats. Continuous patching helps prevent exploitation of known vulnerabilities.

#### 3. Network Segmentation and Monitoring

Isolating IoT devices from other critical systems limits the spread of potential breaches. Real-time monitoring and threat detection further enhance defence.

By integrating these strategies, enterprises can significantly reduce the risk and impact of cybersecurity breaches however these are just three elements. As cyber-attack methods evolve so must the technology, people and processes used within your business. Our [IoT Security Framework](#) is designed to help CISOs, CIOs and System Architects defend, detect and react to IoT cyber-security threats.

### Outages and Recovery

**Outages in IoT deployments disrupt operations, degrade customer trust, and lead to direct financial losses.**

Costs include downtime, loss of productivity, penalties for service-level agreement (SLA) breaches, and expenses for repairs and recovery. Indirect costs, such as reputational damage and customer churn, further escalate the financial impact.

ABB's "Value of Reliability" survey found unplanned outages cost industrial businesses in excess of \$100k per hour, with an eight-hour outage hitting \$1M. Two-thirds face monthly outages, yet 21% still use run-to-fail maintenance.

Unplanned industrial system outages cost businesses \$100K per hour [ABB]



The interconnected nature of IoT systems can amplify these risks, as failures in one component can potentially propagate across networks. Recovery costs increase if outages require manual intervention or on-site repairs, especially in geographically dispersed deployments.

This Wireless Logic whitepaper [Maximising Uptime for IoT - How to achieve high-availability and cyber resilience in IoT](#) provides guidance on how to maximise uptime in IoT including high-availability methods for IoT devices. Three key aspects are summarised below:

#### 1. High-Availability

Implementing redundant systems and failover mechanisms ensures continuity during outages, minimising downtime. This applies to devices, to networks and cloud infrastructure in equal measure.

#### 2. Predictive Maintenance

Using analytics to detect and address issues before they cause outages prevents unplanned downtime and reduces recovery expenses.

#### 3. Proactive Monitoring and Incident Response

Real-time monitoring systems coupled with automated incident response mitigate the severity of outages and accelerate recovery.

By adopting these strategies, businesses can reduce the frequency, duration, and financial impact of outages, ensuring more resilient and cost-effective IoT deployments.

# Capabilities to demand from your IoT Service Provider which will help you reduce TCO



In the first part of this paper, we documented a 12-point framework for identifying and managing the major cost drivers in IoT projects.

In this section we will summarise some of the key technology solutions which Wireless Logic provide our customers to help them manage and reduce costs.



**Myth Busting**  
*Low Power doesn't always mean low cost*



**Application Enablement Platforms (AEPs)**  
*with Low-Code Development*



**Create a single SKU with eSIM & iSIM**



**End-end Solutions**



**Remote SIM Provisioning**



**Fully Managed Services**



**Device Management**



**IoT Security Framework**



**Global 24/7 Operations**



## Myth Busting *Low Power doesn't always mean low cost*

Low power in cellular IoT doesn't always mean low cost primarily because the fragmented network coverage and variation in carrier (MNO) technical and commercial implementations create complexities which can often negate any cost benefits.

These complexities are more acute for international deployments but much diminished for very large-scale regional deployments like smart metering and smart city operations.



### What are these complexities?

#### 1. Fragmented Network Coverage Across Regions

NB-IoT and LTE-M are not consistently available worldwide. Some MNOs support only one technology, and sometimes there is only one network of each type per country. This forces businesses to integrate multiple connectivity solutions. Devices often need dual-mode support, increasing hardware complexity and costs. Coverage gaps may require fallback options, leading to higher operational expenses for global IoT deployments.

#### 2. Variability in Carrier Implementations

MNOs implement NB-IoT and LTE-M differently, with variations in frequency bands, security protocols, and power-saving features. These inconsistencies impact device interoperability, increase testing and certification costs, and require custom firmware updates. Enterprises must invest in region-specific optimisations, complicating deployments and diminishing the expected cost benefits of low-power technologies.

#### 3. International Roaming and Compatibility Issues

NB-IoT and LTE-M do not have widespread roaming agreements, limiting cross-border functionality. Some MNOs charge for or block roaming entirely, requiring local connectivity contracts. Devices may need multi-IMSI, eSIM or carrier-specific adaptations, increasing costs. Certification and regulatory differences further complicate global deployments, making seamless low-power IoT connectivity costly and challenging.

#### 4. Higher Certification and Compliance Costs

IoT devices must meet different country-specific certification and regulatory requirements due to variations in frequency bands and security policies. This results in expensive and time-consuming approvals for multi-region deployments. Additional compliance mandates, such as local security regulations, can drive up costs, making low-power solutions less cost-effective internationally.

#### 5. Complex Supply Chain and Logistics

Region-specific NB-IoT and LTE-M variations force enterprises to maintain different device SKUs, complicating manufacturing, procurement, and distribution. While a single SIM is realistic with multi-IMSI and eSIM, managing multiple modem variants increases logistics costs and inventory risks. Businesses deploying IoT globally must navigate fragmented supply chains, reducing the cost advantages typically associated with low-power IoT devices.

#### 6. Device Lifecycle and Future-Proofing Challenges

NB-IoT and LTE-M technologies are still evolving, and some MNOs may phase out or alter implementations. Enterprises risk deploying devices on networks that may be discontinued, requiring costly upgrades. Future-proofing IoT deployments requires careful planning, often negating the expected long-term savings of low-power cellular technologies.

#### LTE Cat-1 BIS offers a more universal and cost-effective solution for multi-national Enterprise deployments

While careful planning and consultation can resolve some of the complexities described above, there are simpler solutions available which only require very small compromises on hardware cost and battery life.\*

LTE Cat-1 BIS addresses these issues by offering global availability (3, 4 or 5 networks per country) on existing 4G LTE networks, eliminating coverage gaps and roaming restrictions of NB-IoT/LTE-M. It supports a single-radio design, including the SIM which reduces hardware costs and simplifying supply chains. With standardised implementations across MNOs, it minimises certification complexities, ensuring seamless, cost-effective IoT deployments worldwide.

\* Implementation specific. We recommend testing which factors in (i) frequency of communication (ii) data volume (iii) factor in the impact of lower v higher speed (kbps)



Learn more about **Low Power cellular technologies**<sup>†</sup> and why you should partner with Wireless Logic.

<sup>†</sup> including NB-IoT, LTE-M and LTE Cat-1 BIS



## Create a single SKU with eSIM & iSIM

Wireless Logic has been deploying eSIM solutions for more than 10 years and has extensive experience and strong carrier (MNO) partnerships.

The physical security and reliability benefits of embedded eSIMs and integrated iSIMs provide a significant advantage over removable SIM cards. For maximum advantage, OEMs, Solution Providers and Enterprises must also leverage Remote SIM Provisioning (RSP) to manage the full SIM lifecycle from factory to field.

### Standard solution

Our standard SIM solution is a multi-IMSI SIM profile deployed in an eSIM which provides the maximum flexibility and coverage. Multi-IMSI and eSIM mean that updates and localisations can be made via Over-the-Air (OTA) updates. This approach is vital for SKU rationalisation in multi-national IoT deployments.

### Customisation options and advanced functionality

The ability to download and switch IMSI's and SIM profiles OTA provides flexibility and customisation options which can be designed around your business and deployment needs. Wireless Logic has the most expansive carrier eco-system and portfolio of IMSI and eSIM profile partners.

### The key benefits to you

A single SKU eSIM/iSIM with RSP ensures seamless global connectivity, reducing the need for multiple device variants. OTA updates resolve coverage, performance, or compliance issues, including permanent roaming restrictions. This approach simplifies logistics, enhances resilience, and ensures long-term operational efficiency for international IoT deployments.

### Ease and cost of adoption

Wireless Logic supports multi-IMSI and all RSP standards (SGP.02, SGP.22, SGP.32), enabling a streamlined, single SKU approach. This eliminates regional SIM complexities, reducing logistics and operational costs.



Learn more about multi-IMSI, eSIM, iSIM and why you should partner with Wireless Logic.



## Remote SIM Provisioning

To get the full value of eSIM and iSIM technologies, selecting a Remote SIM Provisioning partner with the necessary infrastructure and carrier relationships is vital.

### Standard solution

We partner with best-of-breed RSP and SIM vendors to provide a full-suite of RSP and OTA capabilities which can be used to conduct fleet-wide OTA campaigns or to update individual SIMs or groups of SIMs. This includes updating on-SIM applets, IMSIs and eSIM profiles.

### Customisation options and advanced functionality

OTA campaigns are automated using polling, push, and pull mechanisms, with audit logs and retry strategies ensuring reliability, minimising failures, and optimising global IoT connectivity without manual intervention.

### The key benefits to you

RSP helps Enterprises future-proof their IoT connectivity and maintain a high-level of coverage and resilience over time. Network level or SIM-level changes over-the-air will enable Enterprises to resolve performance, commercial and quality issues should they arise. The rise or government or carrier **restrictions on permanent roaming** means RSP is essential for Enterprises who deploy internationally.

### Ease and cost of adoption

Wireless Logic supports multi-IMSI and all three RSP standards (SGP.02, SGP.22 and SGP.32). We will work with you to identify and automate a solution which suits your business processes and deployment needs. Navigating the RSP eco-system on your own can be complex and expensive so it's important to select and work with a specialist partner like Wireless Logic.



Learn more about Remote SIM Provisioning and why you should partner with Wireless Logic.



## Device Management

Monitoring and Management of IoT devices at a connection, device, security and application level is essential for remote detection and resolution of operational and security incidents.

Managing such events remotely is critical for reducing truck rolls and keeping downtime to an absolute minimum.

### Standard solution

SIMPro is our fifth generation Connectivity Management Platform which has evolved to include Device (DevicePro), Security (NetPro) and Application-level Management (Kheiron). The first lines of defence are Connectivity and Device Management which enable IoT managers to monitor location, frequency, data consumption and can alert, throttle, block or quarantine connections which violate defined parameters.

### Customisation options and advanced functionality

Device Management lets you monitor device health (signal strength, battery levels, temperature) and perform OTA configuration or remedial firmware updates. Kheiron is our Application Enablement platform which include Digital Twin and application data contextualisation and visualisation.

### The key benefits to you

Device Management and Digital Twins minimise truck rolls and downtime by enabling remote monitoring, diagnostics, and predictive maintenance. Digital Twins simulate real-world conditions, identifying potential failures before they occur. Combined with OTA updates and automated issue resolution, enterprises can reduce manual interventions, ensuring optimal IoT device performance and uptime.

### Ease and cost of adoption

Device Management is mandatory for effective management of device security. For industries bound by legislation such as the EU Cyber Resilience Act the cost of non-compliance should not be over-looked. For devices which communicate via standard networking protocols such as HTTPS, SNMP, LwM2M the cost of adoption and integrating into business processes is relatively low.



Learn more about **IoT Management** and why you should partner with Wireless Logic.



## Application Enablement Platforms (AEPs) with Low-Code Development

Historically, the IoT ambitions of many businesses were often blocked by high costs of software development resources or by frustration over the slow or uncertain returns on investment.

Application Enablement Platforms with no-code or low-code development tools reduce the need for large developer teams and/or increases developer productivity.

### Standard solution

Kheiron is a no/low-code platform that simplifies IoT application development with drag-and-drop tools, pre-built integrations, and automation. It enables rapid deployment, reducing development time and costs while ensuring seamless device connectivity and management.

### Customisation options and advanced functionality

For advanced needs, Kheiron offers customised digital twins, dashboard creation and digital twins with enterprise system integration options. For external users and end-customers the dashboards can be pushed to iOS, Android and web-browsers. The platform as a whole can also be white-labelled.

### The key benefits to you

Kheiron reduces costs, accelerates time-to-market, and empowers business users to create solutions without deep coding expertise, enhancing agility and scalability for faster innovation. It accelerates a return on your investment (RoI).

### Ease and cost of adoption

It is easy to get started and scale with Kheiron using a SaaS-based model or run on-premise if you prefer.



Learn more about **Kheiron** and why you should partner with Wireless Logic.

## End-end Solutions

Enterprises increasingly demand end-to-end IoT solutions to reduce complexity, speed up deployment, and lower costs.

Other Enterprises who do have in-house software and system-integration resources the demand is for composable solutions with sensor, hardware and wireless connectivity all pre-integrated.

The cost and time-to-market benefits come from minimising technical overhead especially in areas where skills do not exist in-house, whether that's in the sensor, hardware, connectivity or software domain.

### Standard solution

Our Kheiron IoT Application Enablement Platform reduces development costs and accelerates ROI in a number of ways. This ranges from consultation on sensor and connectivity choices to pre-tested, pre-integrated solutions which can be used to kick-start deployments or to scale Enterprise wide.

### Customisation options and advanced functionality

We cater for customers who need end-end solutions or composable solutions which are essentially building blocks that customers can configure to their own needs and consume on an OPEX basis if desired. Customisation can be done on top of the pre-built application, digital twin and dashboards.

### The key benefits to you

Whether solutions are complete end-end solutions or composable, the need for enterprises to source, integrate, and manage hardware, connectivity, and software from multiple vendors is removed. This counters any knowledge, or resource gaps and reduces risk. Enterprises can test and evaluate ROI before committing to full-scale deployment.

### Ease and cost of adoption

Customers can engage us on a Professional Services basis or consume Kheiron and pre-built solutions on a SaaS or OPEX type model.



**Learn more about Kheiron** and why you should partner with Wireless Logic.

## Fully Managed Services

Performance advances in 4G, 5G and Satellite broadband mean that large enterprises are adopting fully managed Fixed Wireless Access (FWA) services at a growing rate for primary and failover connectivity.

The high speeds of 4G/5G also offer a reliable underlay for SD-WAN deployments, especially in remote areas where fibre lines are not available.

Managing diverse networks, local carriers, and regulatory compliance in-house is complex and resource-intensive, making a single, unified solution essential for operational efficiency and seamless global connectivity

### Standard solution

The 4G, 5G and Starlink based services are designed to provide a hassle-free technical and commercial experience and include cellular-only (4G, 5G) and hybrid (Starlink, 4G, 5G) options over 80 countries globally.

### Customisation options and advanced functionality

The baseline solution and service is designed to be a universally plug and play with customised solutions available when required. We deliver as a fully managed service including hardware (routers, antenna, cabling), installation, device management and optimisation, on-site replacement if required.

### The key benefits to you

Our fully managed FWA service ensures reliable, scalable, and cost-effective connectivity with standardised solutions, proactive monitoring, and automated failover, providing a consistent experience across global branches, regardless of carrier differences or infrastructure challenges.

### Ease and cost of adoption

We simplify global connectivity with a single contract for satellite and cellular, rapid 10-day installation, proactive remote management, and reliable on-site support. Enterprises benefit from seamless procurement, guaranteed uptime, and hassle-free network integration.




**Learn more about Enterprise Connectivity** and why you should partner with Wireless Logic.



## IoT Security Framework

As IoT deployments scale globally, the security risks—from device vulnerabilities to data interception—become more complex. Enterprises are now prioritising end-to-end security frameworks that protect every layer of connectivity, from SIM to cloud.

Wireless Logic's IoT Security Framework offers a unified, embedded approach to securing data and devices across private and public networks, helping organisations meet regulatory compliance while minimising exposure to cyber threats.

### Standard Protection Layer

At the core, our secure connectivity offers encrypted, private networking options including IPsec VPNs, Private APNs, fixed private IP addressing and IMEI locking. These tools work together to provide secure data transit and controlled network access—regardless of SIM location or carrier.

### Advanced controls and integration

Beyond baseline protection, our IoT Security Framework includes advanced capabilities like AI-powered anomaly detection that continuously monitors device behaviour to identify irregular patterns and potential threats in real time. This proactive approach helps mitigate risks before they impact your network or operations.

We also support GSMA's IoT SAFE, enabling hardware-level, certificate-based security by turning the SIM into a secure root of trust. IoT SAFE facilitates mutual authentication and

encrypted data exchange between devices and cloud services, reducing reliance on external security infrastructure and ensuring tamper-resistant protection at scale.

### The key benefits to you

Our IoT Security Framework ensures consistent and scalable protection, tailored to diverse device types and network environments. From real-time visibility and control to full compliance support, enterprises can confidently deploy IoT solutions without compromising security posture.

### Ease and cost of adoption

With security built into every SIM and managed centrally, enterprises avoid the cost and complexity of piecing together third-party solutions. Our unified platform enables fast provisioning, flexible policy updates, and seamless global rollout—accelerating secure IoT adoption at scale.



Learn more about our **IoT Security Framework** and why you should partner with Wireless Logic.



## Global 24/7 Operations

We offer 24/7 Global Operations from our service centres in Asia, Europe and North America.

### Support Excellence as Standard

SIM Assist is a three-tier service designed to meet the demands and budgets of local, regional and global IoT deployments. Access to the 'Wilo' Digital Assistant is included for everyone. 'Wilo' is based on AI/ML/NLP to automate routine service requests and free support agents to deal with the more complex and customer-focussed support services.

SIM Assist Enterprise is designed for blue-chip solution providers, OEMs and Global Enterprise support needs and for dealing with the more complex global deployment challenges. It includes premium features such as quarterly service reviews, 24/7 access to technical support from our Networks & Operations teams and a dedicated care agent.

### The key benefits to you

Our 24/7 Global Operations team and the SIM Assist services is designed to reduce your cost of ownership by keeping your deployment processes streamlined and minimising troubleshooting delays. For example, our onboarding process includes device testing & consultation which is designed to make sure your device will operate as intended in the field. This will ensure your device performs well when roaming, can be controlled over-the-air (OTA) and remain compliant with regulatory controls.

Once deployed, your teams can tap into the expertise of our distributed Network & Operations teams worldwide, who provide localised and real-time support for your IoT deployments. The team is focussed on helping you deploy, scale and maintain high-availability and mission critical solutions.

### Ease and cost of adoption

Select the SIM Assist service tier which suits your project requirements. Global and Mission Critical solution deployments require the SIM Assist Enterprise support tier.



Learn more about how Wireless Logic can help you **create resilient and high-availability solutions.**

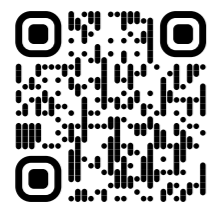
## Contact Wireless Logic

Reliable Connectivity and robust security are fundamental to maintaining operational efficiencies, productivity, safety and security in businesses across all sectors.

Government and industry regulations require increased use of connected devices and are also getting stricter on uptime, cyber-resilience and data privacy.

This paper demonstrates the key role of Communication Service Providers in helping you satisfy those requirements and achieve your desired business outcomes with IoT.

Don't wait until deployment day to think about Connectivity, plan it from the beginning and enlist Wireless Logic as your strategic connectivity partner.



### Contact us...

to discuss any of the content in this guide and receive a breakdown of how Wireless Logic addresses high-availability and cyber-resilience requirements for Enterprises using IoT.



**Certificate Number 19387**  
ISO 9001, ISO 22301, ISO 27001  
ISO 14001, ISO 50001

*Thank you for connecting  
with Wireless Logic.*



**Wireless Logic Group Ltd**

4th Floor, The Davidson Building, Forbury Square, Reading, RG1 3EU, United Kingdom

Call: +44 (0)330 056 3300

Email: [hello@wirelesslogic.com](mailto:hello@wirelesslogic.com)

Web: [wirelesslogic.com/conexa](http://wirelesslogic.com/conexa)

---

**Other office locations**

<b>Australia</b>	<b>Germany</b>	<b>North America</b>
<b>Austria</b>	<b>Italy</b>	<b>Norway</b>
<b>China</b>	<b>Liechtenstein</b>	<b>Singapore</b>
<b>Denmark</b>	<b>Malaysia</b>	<b>South America</b>
<b>France</b>	<b>Netherlands</b>	<b>Spain</b>

**wirelesslogic.com**

