WIRELESS LOGIC **WHITEPAPER**

wireless logic

An IoT Security Framework for Enterprises and OEMs

Creating competitive advantage and cyber-security compliance

wirelesslogic.com

Why Business Leaders must **prioritise Cyber-Security Compliance**

Businesses and IoT are under attack

1. The average cost of a data breach is increasing YoY ($5M EU, $10M US)
2. The average time taken to detect security breaches is ~200 days
3. One in three data breaches now involves an IoT device.
4. 15% of breaches involved third-party technology
5. Unpatched firmware is responsible for 60% of IoT security breaches.
6. The Mirai botnet turned unsecured IoT devices into an army of attack machines, launching one of the biggest DDoS attacks ever recorded.

As cyber threats targeting IoT systems grow in scale and sophistication, CIOs, CISOs, Chief Product Officers, and Product Managers must move beyond static best practices. Tackling this evolving threat landscape demands that senior leadership secure appropriate funding, resources, and governance across their supply chains and within their organisations' technologies, people, and processes.

Maintaining both defensive and proactive security across connected devices, communication networks, data flows, and application layers is no longer optional. The rise of ransomware, malware, device spoofing, and man-in-the-middle attacks poses severe operational, financial, safety, and reputational risks to enterprises.

This challenge is intensified by the expanding scope and stringency of cyber-security legislation, which places greater legal and regulatory responsibility on leadership teams to demonstrate continuous due diligence and compliance.

The Wireless Logic IoT Security Framework offers a comprehensive, 360-degree approach to mitigating these risks. Its Defend, Detect, and React methodology spans people, processes, regulatory alignment, and advanced technologies—such as intelligent SIMs, private networks, and AI-powered threat detection. This equips enterprises not only to manage today's cyber risks but also to meet the demands of an increasingly regulated digital future where minimising service disruption, demonstrating compliance and providing evidence of robust security measures to regulators is essential for IoT-enabled businesses.

Use the IoT Security Framework to help you differentiate and win more business while also avoiding the full force of regulatory investigation and fines should you suffer a breach.

Sources : IBM (1-2), Verizon DBIR (3-4), IoTSF (4), Kaspersky (6)

Contents

Defend
Manage your cyber-attack surface to prevent unauthorised access to devices, cloud infrastructure and data.

Detect
Leverage usage based insights and detailed analysis of device and network behaviour to detect cyber threats.

React
Apply automated counter-measures against problem devices and systems to isolate security breaches and take remedial action.

Return to Contents

The rapidly evolving legislation and regulatory landscape

The legislative and regulatory landscape covering IoT cyber-security is evolving fast across the globe.

- The EU and UK have the most integrated and binding product-level cybersecurity regimes including EU CRA, NIS2, EN303645 and EN18031.
- The USA is more sectoral and fragmented but driven by robust NIST technical frameworks.
- LATAM is evolving, mainly through data laws and early-stage infrastructure policies.
- China enforces cybersecurity with strict controls and certification regimes.
- Asia-Pacific blends voluntary-to-mandatory schemes with high alignment to EN 303 645.

Case Study The Cyber Security landscape in EU

The **EU Cyber Resilience Act (CRA), NIS2 Directive, EN 18031,** and **EN 303 645** are all part of the evolving European regulatory and standardisation landscape aiming to improve **cybersecurity across digital products and networks.** While they overlap in objectives, they differ in **scope, legal nature,** and **application**.

Here's how they relate:

Regulation / Standard	Legal Status	Scope	Role / Focus	Related To
CRA	Regulation (EU law)	All digital products	Product cybersecurity across lifecycle	EN 303 645, EN 18031
NIS2	Directive (EU law)	Critical sectors & operators	Organisational cyber risk management	CRA
EN 18031	Harmonised Standard	Internet-connected radio devices	RED compliance (cybersecurity for wireless devices)	EN 303 645, CRA
EN 303 645	Technical Spec	Consumer IoT devices	Security baseline, best practices	Basis for EN 18031, CRA

EN 18031 in particular has far reaching implications for Enterprises and Original Equipment Manufacturers (OEMs). The UK's **Cyber Security and Resilience (CS&R) Bill** aligns well with **EN 18031**, although not fully harmonised.

Compliance with **EN 18031** is crucial for access to the European market - **non-compliant devices will be deemed unsafe and will not receive a CE Mark.** This means they cannot be legally used or sold in the European Economic Area.

The standard emphasises three new essential cyber security requirements for IoT devices, as defined by **Commission Delegated Regulation (EU) 2022/30**—also known as the **RED Delegated Act** or most commonly as **Radio Equipment Directive.**

Navigating new IoT cyber security standards

Understand the impact of EN 18031 and the UK CS&R Bill on IoT security, compliance and market access requirements.

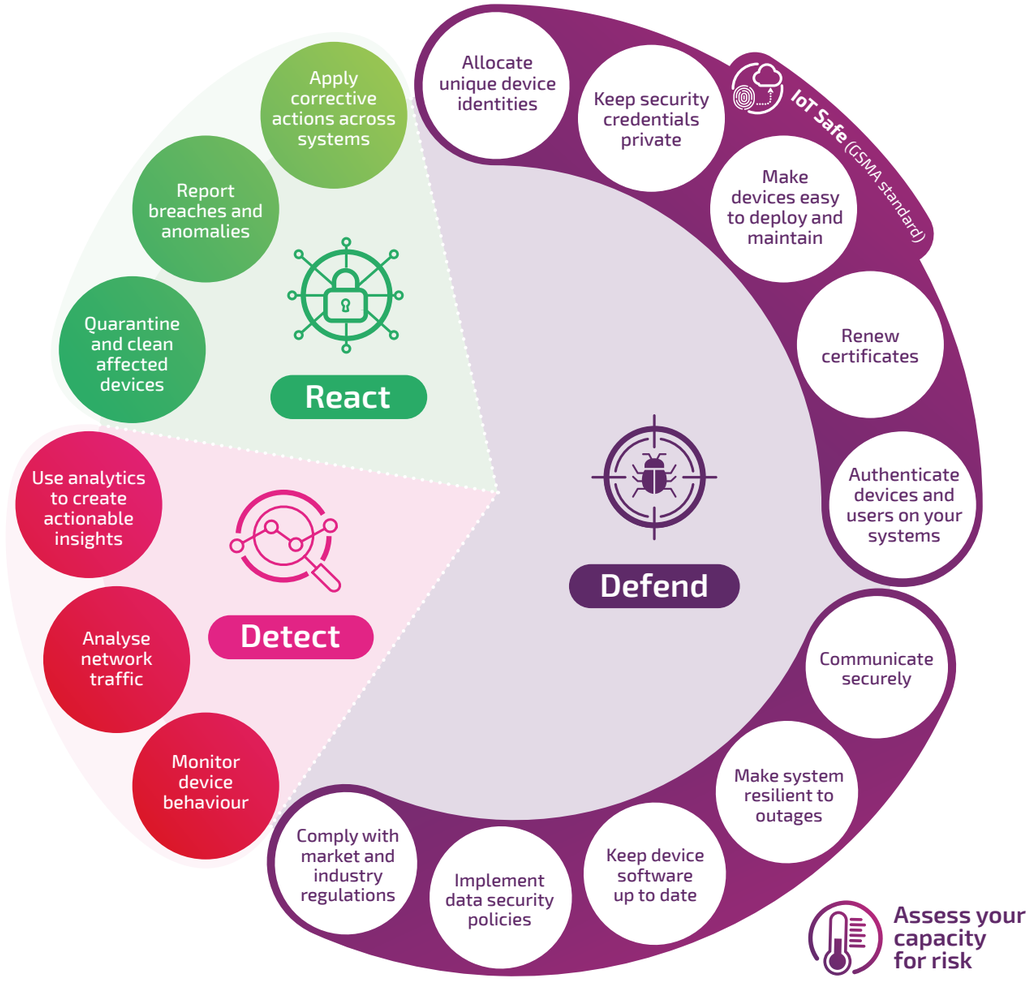
- **Network protection (3(3)(d)):** Devices must not harm the network or misuse network resources. They must be built to prevent cyber-attacks and ensure the integrity of connected networks.
- **Privacy protection (3(3)(e)):** Devices must ensure the protection of personal data, aligning with privacy laws like GDPR to safeguard user information.
- **Fraud prevention (3(3)(f)):** Devices must incorporate features to prevent fraudulent activities, such as unauthorised access or data manipulation.

Return to Contents

Wireless Logic **IoT Security Framework**

The framework consists of 16 provisions which help Enterprises defend, detect and react against IoT cyber-security threats.

The framework provisions map well to standards like ETSI EN 303 645 or NIST CSF enable IoT device manufacturers and solution providers to make their cellular IoT solutions secure by design.



The framework also helps assess capacity for risk.
The appropriate level of security might be dictated by your customers or standards or by your assessment of acceptable risk and a trade-off between other factors such as price, compute resource or ease-of-use.

How to use the IoT Security Framework

The IoT Security framework is built around a Defend, Detect, and React methodology which contain guidance on people, processes, regulatory alignment and advanced technologies - such as intelligent SIMs, private networks, and AI-powered threat detection.

We want to work with you to assess which provisions are most critical for your business and your industry. The process and recommendations will vary depending on what stage you are at and how you have built or plan to build your solutions.

1 I will buy IoT devices from 3rd party suppliers and integrate them.

Build your RFI processes using the framework and assess device suppliers and other service providers on how well they understand and satisfy cyber-security requirements.

2 I am developing my entire solution including devices and network in-house.

Even when you are developing in-house you will still procure things like software development tools and electronic components including cellular modules and SIMs. Use the framework to help your teams develop security in from the start and also to assess security credentials of suppliers.

3 I have already deployed my IoT solution and need to retrofit security.

This does makes it more difficult to adopt some security technologies especially where deployed hardware is involved. In many cases, it is still possible however to transfer SIMs to different connectivity providers and retro-fit security, including Anomaly & Threat Detection.

Return to Contents

Not if, but when?

Cyber-criminals continue to innovate at pace and are using automation in very creative ways to probe for network and IT weaknesses. Likewise, AI has been employed by cyber-criminals to fish for system credentials from unsuspecting staff members.

So even with the best made defences, cyber-security breaches in the IoT space are not a matter of *if*, but *when?*

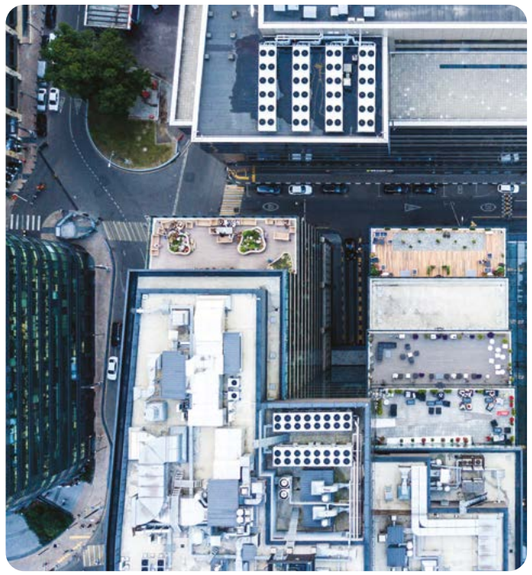
Technology plays a vital role in cyber-resilience, but businesses must also invest in People, Processes, and Simulation. Doing so will significantly reduce their exposure by adopting a proactive security posture that emphasises investment in training, processes, and realistic simulation.

People are the first line of defence. Investing in continuous education ensures employees remain alert to evolving threats and understand their role in upholding security. Cyber-awareness training can help mitigate risks stemming from human error, which remains one of the most common breach vectors.

Processes provide a structured approach to threat prevention and incident response. Establishing clear protocols—such as access controls, risk assessments, and data handling procedures—ensures that security is built into day-to-day operations rather than bolted on as an afterthought.

Simulation plays a vital role in exposing weaknesses before real attackers can exploit them. By regularly running penetration tests and red team/blue team exercises, businesses can assess their defences, train their teams under pressure, and adapt their strategies accordingly.

Ultimately, effective cyber-resilience is not static. It requires continuous rehearsal and iteration. Businesses that invest wisely in these three areas are not just protecting assets—they are building agility and trust into the core of their digital operations.



The average time taken to detect security breaches is 200 days

Read on for 3 case studies which provide examples of how investment technology, people and processes can reduce the time to detect and react to cyber-attacks and breaches.

Case Study
Be prepared by simulating a cyber-attack

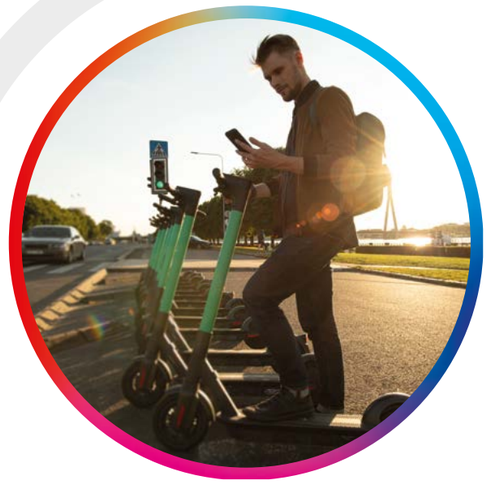
Tools that simulate security attacks help businesses to rehearse how they will respond and act, in the event of an actual incident.

Specialist companies also offer workshops during which they will present a 'what if?' mocked-up situation. These are specific to the organisation and IoT solution, with scenarios that map to the applications and systems the business uses. They will facilitate a detailed walk through of the steps the company should take to deal with such a situation. All of which provides valuable insight.

It is important that businesses have a ransomware strategy and rehearse how they would react to a ransomware event. There are questions to consider here, including whether or not to pay in the event of a ransom demand, and whether to take out ransomware insurance.

If going down the insurance route, businesses should be clear on if it will cover only the cost of the ransom. There are additional potential costs that could be incurred, such as those involved in resolving an issue and revenue, and possibly reputational damage.

A business in the midst of dealing with a ransomware attack should not be considering these important choices for the first time. They should think through what they would do in advance and prepare for and practise potential attacks.



Return to Contents

Case Study
How to monitor cellular devices outside of the IT perimeter

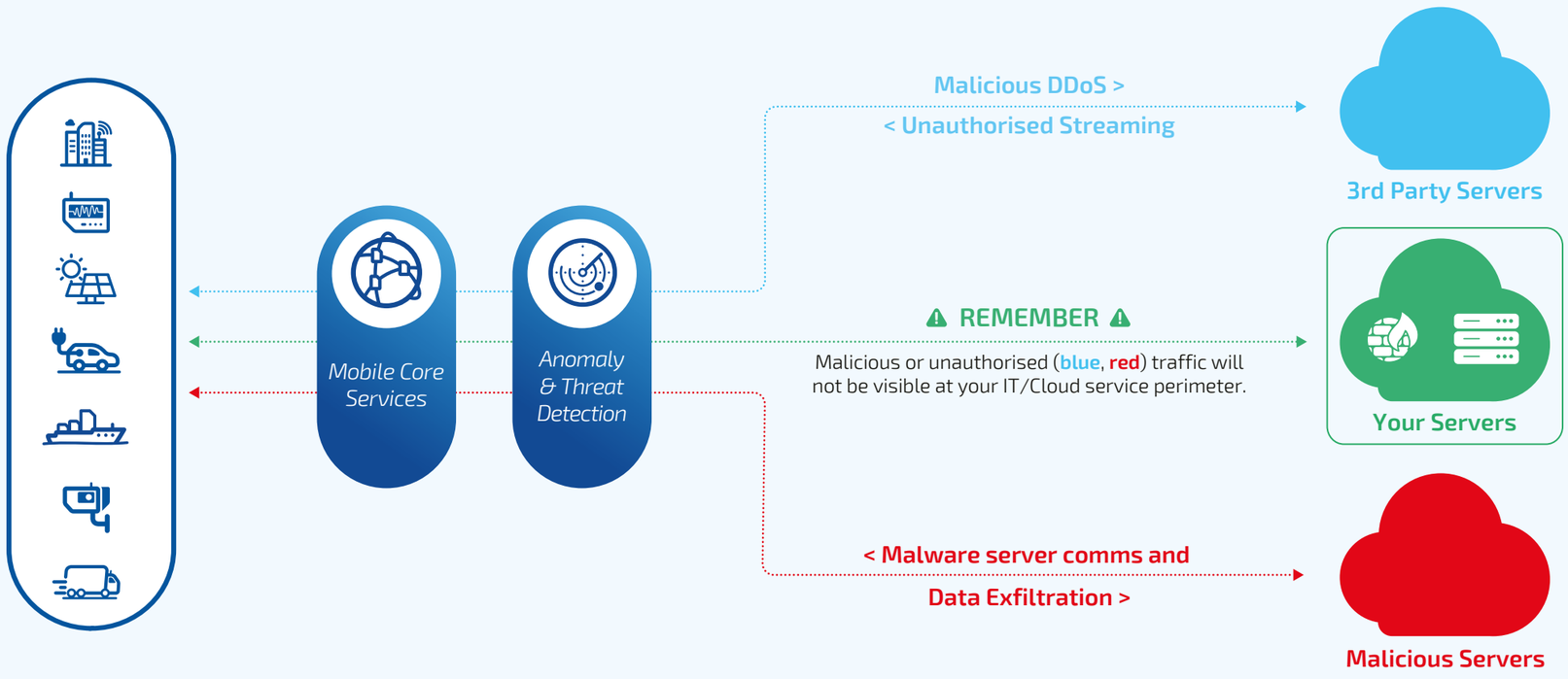
Monitoring device behaviour beyond the standard IT perimeter is essential for compliance with cyber-security legislation, which increasingly requires organisations to detect and respond to anomalous activity across all endpoints.

While Cloud Service Providers and conventional IT solutions are effective at securing the core network and guarding the perimeter, they typically do not extend visibility to edge or remote devices—especially IoT endpoints or embedded systems. (This is indicated in the green box around the green server/cloud in Figure 1). As a result, threats such as IP backdoors, malware communications, or attacks on third-party servers may go undetected.

These threats often originate from compromised devices operating outside direct IT control, where traditional defences offer no insight. One indirect indicator of compromise—such as a Mirai-style infection—might be unexpected spikes in data usage, which will be flagged by alerts from Connectivity Management Platforms (CMP or SIMPro) or will appear in billing data at the next billing cycle.

However, CMP alerts and billing indicators are reactive at best. In contrast, Anomaly & Threat Detection provides pre-emptive or real-time insights into the spike in data usage and the likely causes.

Figure 1:
Monitoring devices which are 'out of perimeter' will help detect usage of 'backdoors' and malware attacks.



Case Study
How to detect 'IP backdoors' and Mirai botnet

Since the Anomaly & Threat Detection function runs entirely in the mobile core network infrastructure and without any device software agents it can be retrofitted to existing deployed systems.

Within hours, customers have identified 'IP backdoors' and Mirai botnet infections on IoT devices by detecting deviations from normal network behaviour. (In figure 1, this is indicated by the red and blue server/clouds.)

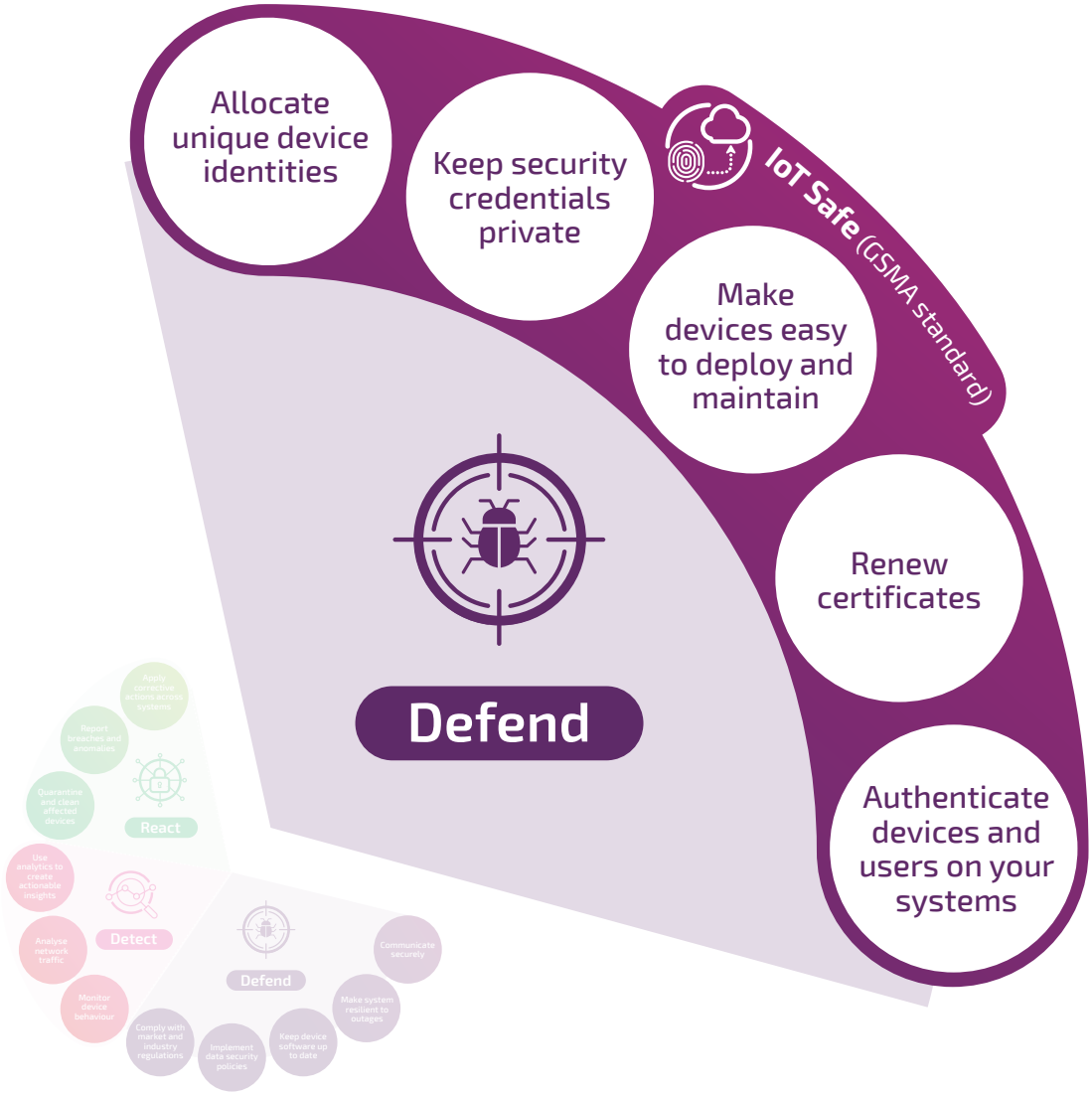
For IP backdoors, these methods detect unusual outbound connections or traffic to suspicious IPs that deviate from expected communication patterns of the device. Such backdoors may allow remote control or data exfiltration, both of which leave identifiable behavioural traces.

In the case of Mirai, infected IoT devices typically exhibit spikes in outbound traffic, use of uncommon ports, or repetitive scanning of external IPs—activities that diverge from their baseline functions.

By using statistical models, machine learning, rule-based algorithms or AI, Anomaly & Threat Detection systems can flag these irregularities in real-time and corrective actions can be identified and implemented. Corrective actions could include blocking devices, quarantining device, blocking or throttling of traffic and device firmware patching.

Defend against cyber threats

Part 1 *Manage identity*

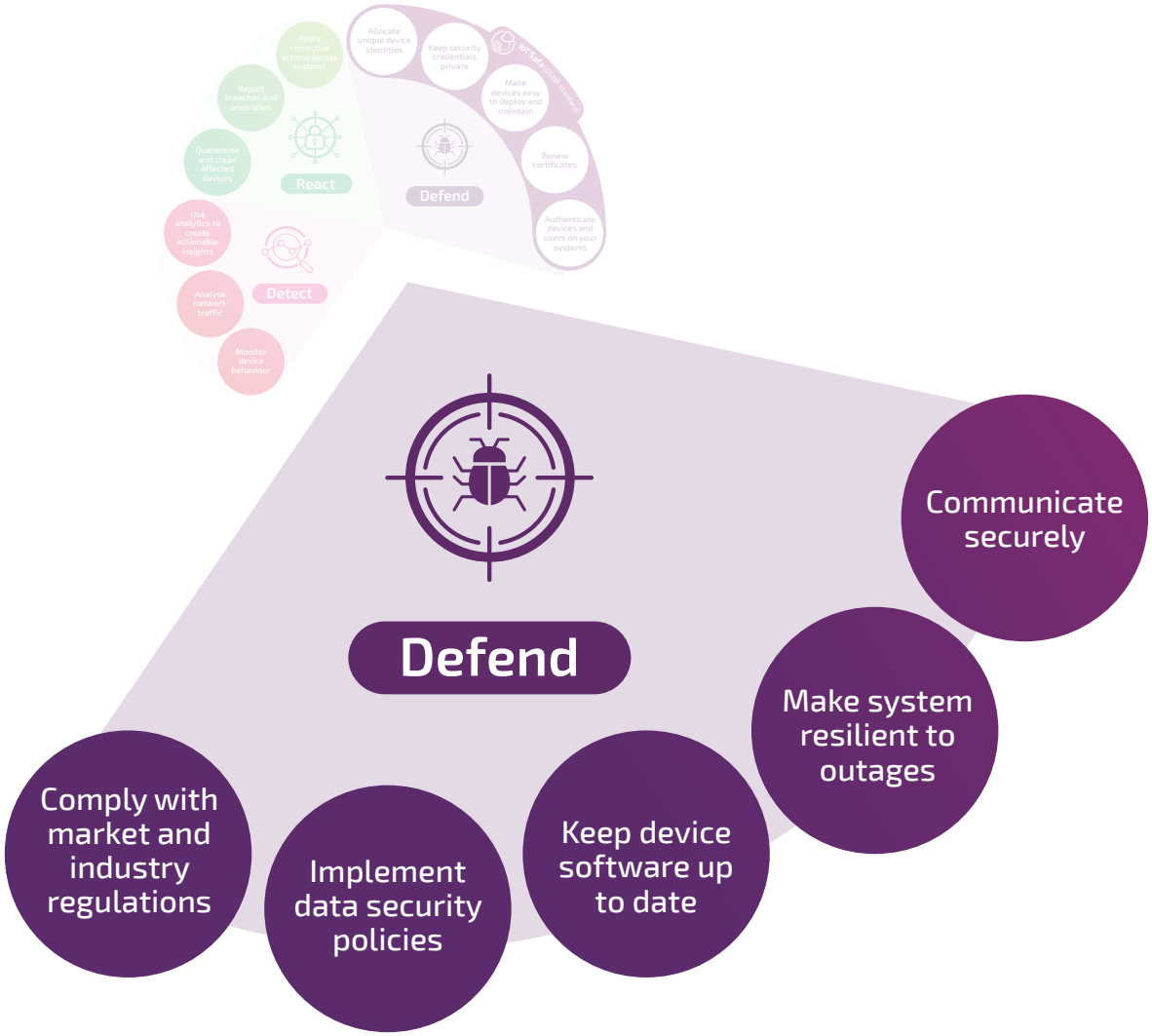


End-to-end authentication with IoT Safe?

- Zero Touch Provisioning: wake up, connect, authenticate, communicate
- Remove security hardware overhead in your devices
- Cloud Portability. Lower cost certificate provisioning
- Reduced security complexity
- Evolve your security approach over time as new products are launched and threat

Defend against cyber threats

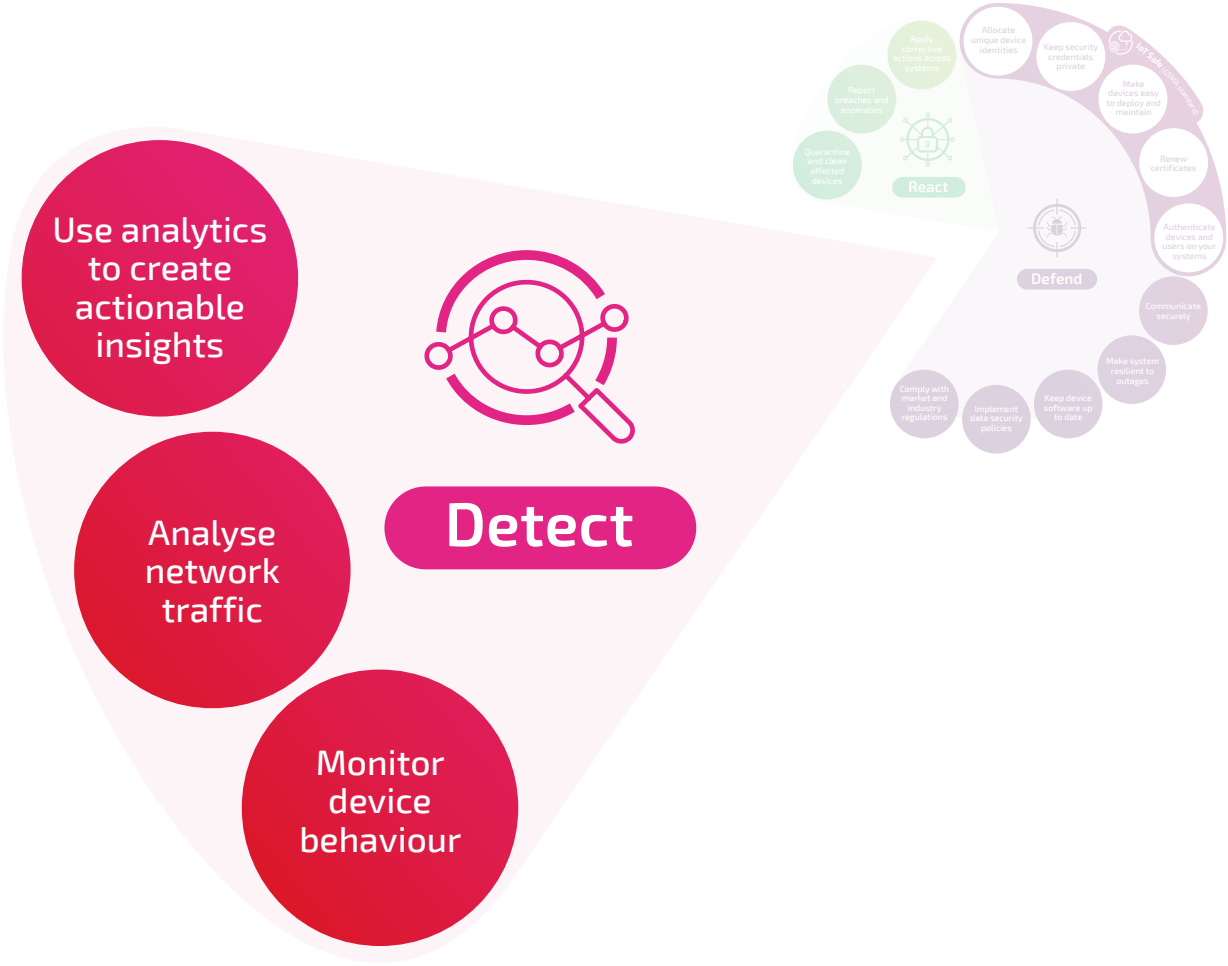
Part 2 *System resilience, people and processes*



The non-negotiables

- Insist on high-availability and cyber-resilient solutions from your connectivity and cloud providers
- Implement secure and redundant/resilient interconnects
- Invest in People, Processes and Partners - these might be your biggest security risk
- Choose partners with a strong reputation and security credentials

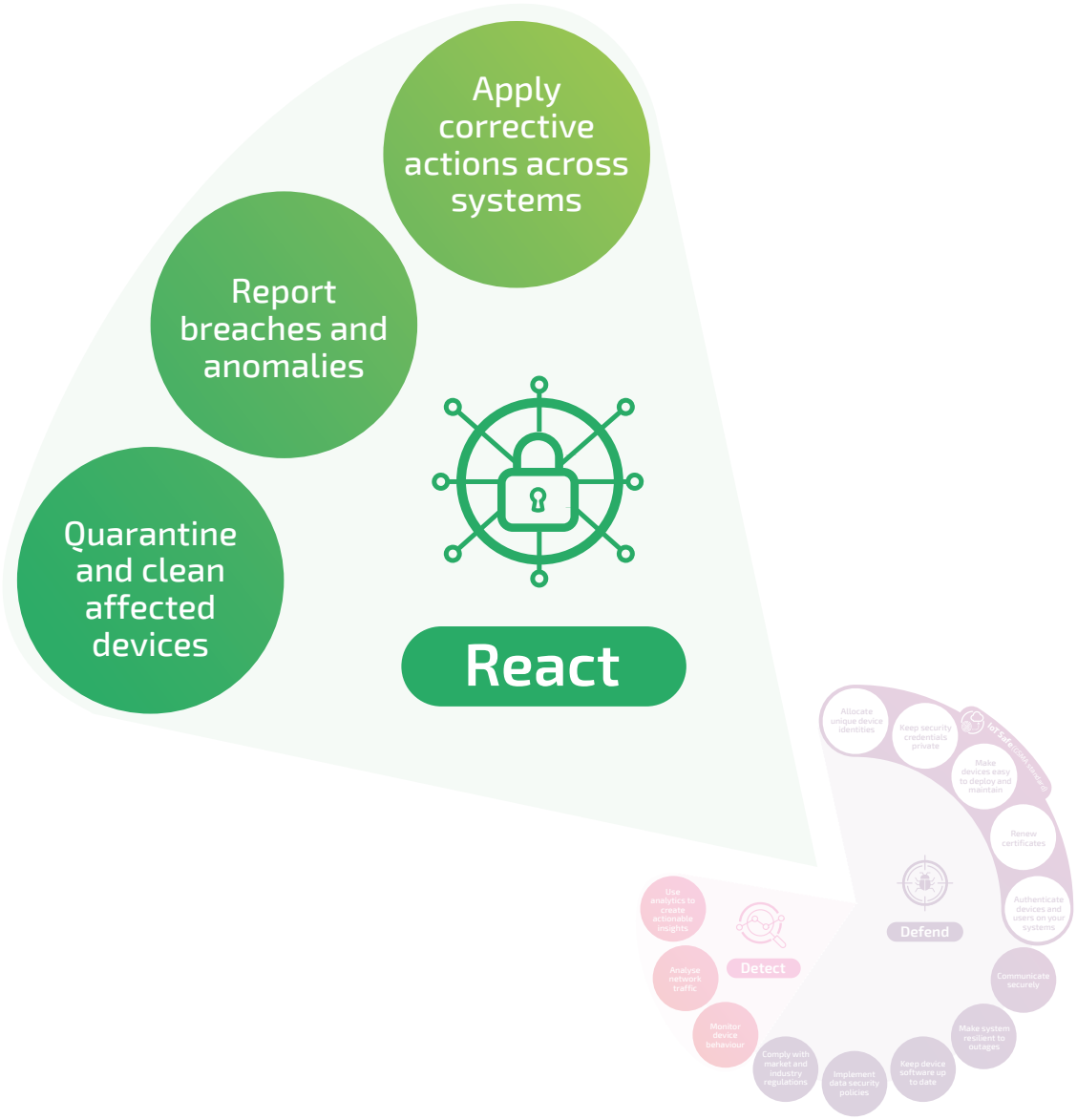
Detect threats using pre-emptive cyber security



How does real-time Anomaly & Threat Detection work?

- Profile your IoT network baseline behaviour
- Monitor device, network traffic and application level behaviour
- Real-time Alerts and Automate responses
- Granular, single device or fleet, system-wide updates and controls

React quickly to isolate security breaches and take remedial action



Prepare your systems to react to security breaches

- Model and optimise your solution at start of the design before deployment
- Manage device behaviour, tweak configuration over the air
- React automatically to device changes by terminating connectivity or alerting for investigation
- Apply corrective actions across all systems including customers and partners if required

The **Wireless Logic IoT Security Stack**

Identity Management
Robust authentication and privacy measures, including IoT SAFE, ensure that only authorised devices can connect to your networks.

High-Availability Core Functions and Interconnects
Minimise interventions by leveraging IoT core network infrastructure designed specifically for secure and resilient IoT operations.

Secure Private Networking
Private APN and VPN services provide secure and resilient private networking between our infrastructure and your systems and people.

Connectivity Management
Monitor your device fleet and implement lifecycle management processes on our Connectivity Management Platform.

Device Management
Implement regular firmware patching and device monitoring to defend against cyber-attacks or remediate device-level breaches.

Application Development
Application level monitoring and alerting provides an additional layer of defend and detect capability.

Anomaly & Threat Detection
Monitor device to cloud end-point communication and highlight deviations from normal behaviour.

24/7 Global Operations
24/7 monitoring, alerting and reporting of device, network behaviour and security threats.

Return to Contents

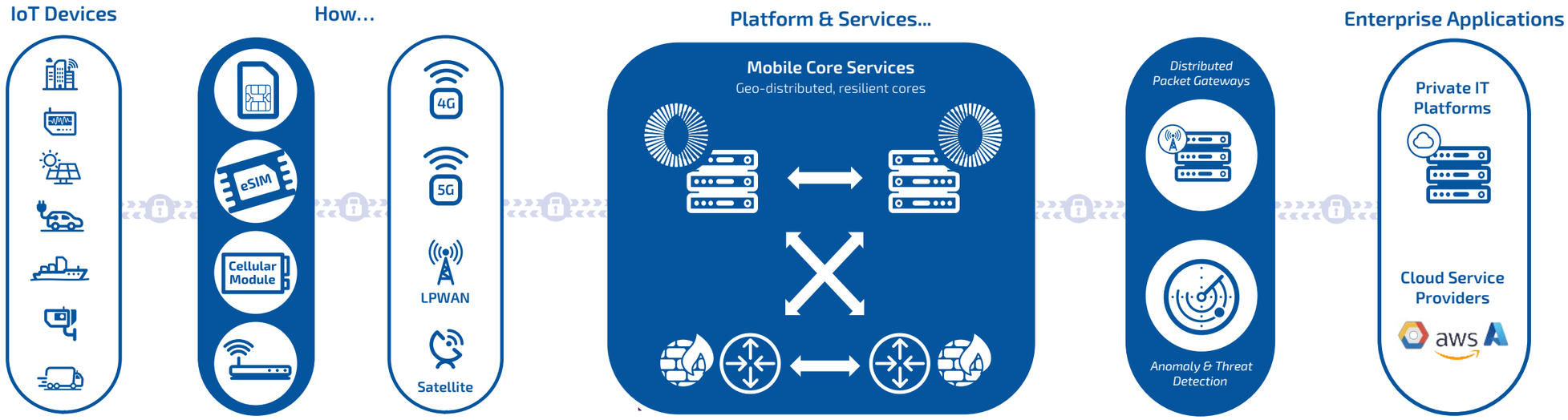
Mapping our security stack to device – network - cloud based IoT systems

Key

Where functions are implemented and scope of operation

Extended scope of services

Device/user interactions or control interfaces



Identity Management

- Private IP Addressing to isolate devices from public internet
- SIM-based Authentication for mobile network access
- Lock SIM and Device hardware IDs to prevent fraudulent usage (IMEI Locking)

Certificate-based Authentication (IoT SAFE) with cloud/ enterprise-based applications.

High-Availability Core Functions and Secure Interconnects

Wireless Logic operates a dedicated IoT core network designed and built for IoT. The core functions run on secure and geographically dispersed data centre infrastructure with separate power supplies to ensure reliability and resilience.

Secure Private Networking

Secure private networking solutions to prevent data theft, ransomware, malware and man in the middle attacks.

- Carrier encryption
- Private IP and APN
- IP safe-listing
- IP-based encryption (eg TLS)

IPSec & SSL VPN for secure data and remote user access.

IoT Management

Monitoring and Management of IoT devices at a connection, device, security and application level is essential for detection and resolution of operational and security incidents. Measures include IMEI-locking, IP safe-listing, blocking, capping, throttling, firmware patching and more.

Digital Twin and data visualisation capabilities provide application level monitoring and management.

Automate responses and threat prevention measure through tighter integration with your business and IoT Management systems

Anomaly & Threat Detection

Pre-emptive cyber security breaches through AI-based monitoring od device to cloud/server communication behaviours.

Compliance Reports support industry and government regulation requirements.

24/7 Global Operations

24/7 monitoring, alerting and reporting of device, network behaviour and security threats. Our NOC/SOC operations operate from our service centres in Asia, Europe and Americas.

Device Authentication and Identity Management

A unique and immutable device identify is essential for preventing impersonation or spoofing. In other words, to ensure that only authorised devices are communicating with your servers.

We solve this while also enabling you to reach devices from your servers using a series of measures described below.

Standard Solution

We advocate the use of private IP addresses in addition to SIM based authentication. These measures combine with Private APN and VPN to separate and secure your device traffic from regular internet traffic and the threats which can exist there. If a public IP address is really required by your industry or your customer's, then we have solutions which improve the security of those public IP endpoints.

Customisation Options and Advanced Functionality

Use the SIM to store and distribute certificates and automate PKI creation and maintenance using our standards-based, secure IoT SAFE infrastructure. IoT SAFE is a GSMA standard which enables the certificate-based security used in contactless payments, mobile and IT industries to be implemented on IoT devices.

The key benefits to you

Robust authentication and identity management defends your network against spoofing, ransomware attacks and unauthorised network access which can lead to service loss or device/network downtime.

Ease and Cost of adoption

We provide private IP and APN solutions as standard. Enterprise adoption of IoT SAFE requires some planning and collaboration with OEM/ODM and Cloud/Server teams but it is otherwise very cost-effective and can produce savings on bill-of-materials, support hybrid cloud environments and reduce the cost of ownership on identity (certificate) management.

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

High-Availability Core Functions and Interconnects

Wireless Logic operates a dedicated IoT core network designed and built for IoT.

This is in addition to carrier partner core and radio network infrastructure. In all cases, the core functions run on geographically dispersed data centre infrastructure with separate power supplies to ensure reliability and resilience.

Standard Solution

Our Core infrastructure operates in an active-active, mode ensuring that there is a continuous view of the health of our systems and a failover available for all traffic in the event of service degradation. Time to restoration of service if device needs to establish a new connection is automatically handled by directing traffic to the active node with no manual intervention required.

Customisation Options and Advanced Functionality

We also operate a network of distributed Packet Gateways to provide localised and low latency data connections to Enterprise network or internet services.

We advocate dual-IP addresses for devices and map those to redundant packet gateways to automate failover and outage recovery processes should an outage occur.

The key benefits to you

Our mission-critical applications are structured as microservices and run on Kubernetes clusters, strategically positioned across multiple data centres. The active-active setup ensures high availability and reliability while minimising the risk of downtime.

Ease and Cost of adoption

Mapping of traffic between core and regional packet gateways requires advance planning but adoption of Conexa is otherwise seamless. If dual-IP addresses are used then servers must resolve using DNS before contacting remote devices.

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

Secure Private Networking

More than 95% of IoT connections managed by Wireless Logic use NetPro, our Private APN and VPN services infrastructure.

NetPro services form a critical part of your defence against security threats and combine with carrier encryptions and IP-based encryption protocols such as TLS to provide end-end encryption of data in transit.

Standard Solution

We advocate Private APNs as standard. An APN is a gateway which enables IoT devices to use mobile network infrastructure to connect to enterprise networks, without having to access the public internet. Our NetPro infrastructure includes high-capacity fibre links to carrier networks and is implemented in geo-resilient data centres to maximise reliability.

Customisation Options and Advanced Functionality

IPSec VPNs are typical for site-site VPNs (connecting Wireless Logic to Enterprise infrastructure) and SSL VPNs for ad-hoc remote access. Unless you are already using end-end TLS encryption on your device-server traffic, IPSec VPNs are essential.

The key benefits to you

Use secure private networking solutions to prevent data theft, ransomware, malware and man in the middle attacks and protect your brand and reputation

Ease and Cost of adoption

Private APNs and carrier encryption comes as standard, VPNs require some planning between NetOps teams on each side but should be used in all but a few cases where the simplest binary (on/off) or sensor data is being transmitted. See ***Device Authentication and Identity Management*** for details on cost-effective TLS implementation in IoT.

Learn more about Secure Private Networking and why you should partner with Wireless Logic.

IoT Management Platform - Connectivity, Device, Application

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

This includes detection of unauthorised data consumption, location, device health and system or application level anomalies. Real-time detection and pro-active reactions will be critical for preventing wide-spread loss of service and outages.

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 line of defence is SIMPro which monitors location, frequency and volume of consumption and can alert, throttle, block or quarantine connections which violate your defined parameters.

Customisation Options and Advanced Functionality

DevicePro lets you monitor device health (signal strength, battery levels, temperature) and perform OTA configuration or firmware updates. Kheiron is our Application Enablement platform which include Digital Twin and application data contextualisation and visualisation with, mobile push notifications, SMS and email alerting.

See also ***Anomaly & Threat Detection***

The key benefits to you

A 2022 IBM data security report identified that the average time to detect and report a security breach was around 9 months. Real-time multi-level monitoring is crucial to accelerate detection and remedial action and to minimise the damage caused by operational or cyber-security incidents.

Ease and Cost of adoption

These services are mandatory. Enterprises should apply connectivity, device, security and application-level monitoring according to their risk profile and tolerance to service or data loss/corruption.

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

Anomaly & Threat Detection (ATD)

Solution Providers, IT/OT System Integrators and end-user Enterprises use Anomaly & Threat Detection to identify the first signs of cyber-attacks against their IoT systems.

It also provides them with threat management measures, operational visibility and supports their compliance efforts with industry and government regulators.

Standard Solution

Packet headers from device-cloud communications can be mirrored from our mobile core to our Anomaly and Threat Detection engine for near real-time AI-driven analysis with insights and threat levels communicated via the UI for investigation and remedial action. These processes will alert you to abnormal usage or end-point communications and provides warnings of malware, ransomware events.

Customisation Options and Advanced Functionality

Service extensions are also available to support tighter integration with your business systems and automation of responses, threat prevention and the production of compliance reports. These reports will provide important evidence of the monitoring and prevention measures you have in place which is information government regulators will seek should you ever experience a security breach.

The key benefits to you

If left undetected or unresolved, cyber-attacks can lead to chronic operational challenges, loss of reputation and financial penalties. Anomaly and Threat Detection reduces this risk and provides vital evidence of your monitoring strategy should you need to demonstrate to regulators.

Ease and Cost of adoption

Deployment of Anomaly and Threat Detection is seamless. It does not require any software agents to be installed on IoT devices and does not compromise your system performance or data privacy commitments.

Learn more about Anomaly & Threat Detection and why you should partner with Wireless Logic.

24/7 Global Operations

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

SIM Assist is our comprehensive support solution which includes the "Wilo" Digital Assistant 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.

Standard Solution

SIM Assist is a three-tier service and includes SIM Assist Enterprise designed for blue-chip solution provides, OEMs and Enterprises. It delivers expert help for the most complex solutions, including 24/7 support for P1 and P2 incidents.

SIM Assist Enterprise features the fastest SLAs for first response times across all tiers and includes premium features such as proactive incident reporting, root cause analysis reporting for P1 incidents and a dedicated care agent.

The key benefits to you

Once you have onboarded as a customer you can tap into the expertise of our distributed Service and 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 solutions.

Ease and Cost of adoption

Our service tiers are designed to meet the demands and budgets of local, regional and global IoT deployments.

Learn more about 24/7 Global Operations and why you should partner with Wireless Logic.

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 security and connectivity, plan them 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.

Contact us

Wireless Logic Group Ltd
Horizon, Honey Lane, Hurley, Berkshire SL6 6RJ, UK
Call: +44 (0)330 056 3300
Email: hello@wirelesslogic.com
Web: wirelesslogic.com/conexa

Other office locations

Austria
China
Denmark
France
Germany
Italy
Netherlands
Norway
Spain
USA

wirelesslogic.com