
# Anomaly & Threat Detection

## IoT Device Intelligence and Threat Management

**Anomaly & Threat Detection is a Wireless Logic solution for CISOs, CIOs and Product or Operations Managers seeking to maximise value and utilisation of IoT devices and protect the Enterprise IT domains from external threats.**

IoT devices typically operate in environments outside of the traditional Enterprise IT perimeter and in huge quantities. Until recently, this made them more susceptible to cyber-crime and more difficult to monitor and manage.

Our Anomaly & Threat Detection (ATD) solution delivers a pre-emptive cyber-security capability which monitors IoT device behaviour and traffic directly in the mobile core network.

Powered by AI, it provides visibility and actionability for out-of-perimeter cellular IoT devices without any need for software agents on devices.

***Strategic investment in pre-emptive cyber-security solutions is essential and cost-effective when compared to the potential consequences of:***

- *Unplanned operational downtime*
- *Regulatory penalties*
- *Reputational harm*
- *Unexpected data consumption*

*The benefits of Anomaly & Threat Detection* >

# Safeguarding performance, compliance, and brand reputation in a connected world

**The current threat landscape represents a significant business risk. While technology in your devices, networks and cloud systems provide a strong line of defence, cyber-criminal methods are constantly evolving and making use of AI to automate frequency and scale of phishing attacks against your employees.**

- *1 in 3 breaches involve IoT endpoints (Verizon DBIR)*
- *200 days: average time to detect a breach (IBM)*
- *Regulatory frameworks tightening: EN 18031, CRA, NIST CSF*
- *Global impact: Compliance applies beyond regional borders*
- *Communication frequency changes*
- *Zero data usage (devices are offline)*
- *Abnormal downloads*
- *Higher volume data transmissions*
- *Communication with unusual server endpoints*

**Impact of non-detection**

### Financial Losses
*Breaches cost money. There may be a need to investigate the cause, recover systems, install new security measures, pay fines or ransoms and seek expert assistance.*

### Reputation Damage
*A breach undermines trust. Customers, partners, and stakeholders lose faith in the company's ability to protect information, leading to business loss and reputation damage.*

### Data theft
*Sensitive data exposure in a breach can lead to identity theft, fraud and cybercrime incurring more financial losses and legal liabilities.*

### Operational Disruption
*Breaches can lead to downtime as systems are investigated, cleaned, and restored. This can disrupt normal business operations, impacting productivity and revenue generation.*

### Regulatory Consequences
*Industries face stringent data protection regulations. A breach can lead to non-compliance, resulting in fines, penalties, and legal consequences.*

## Framework for assurance

**Defend**

**Identity management, SIM-authentication, secure networking**

**Detect**

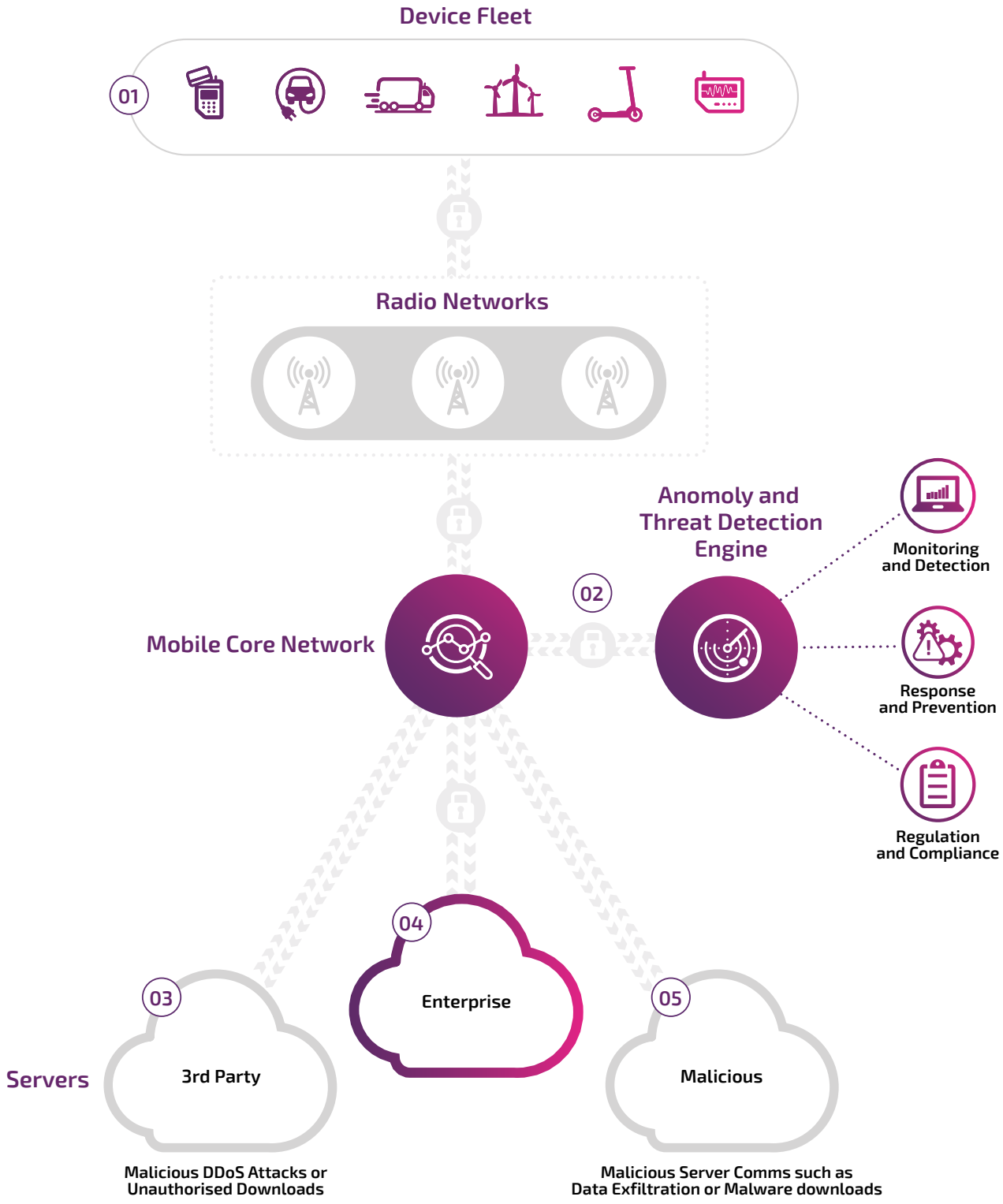
**AI-driven monitoring of network behaviour and traffic**

**React**

**Automated isolation and remediation across systems**

*What can ATD detect and how?*

# How Anomaly & Threat Detection works...




*01* *Devices can be offline due to malfunction or ransomware. They can be taken over by cyber criminals and used to launch DDoS attacks*

*02* *Constant monitoring in our mobile core network will detect traffic anomalies and other unusual device behaviour.*

*03* *Unauthorised device usage or compromised devices can communicate with or attack 3rd party servers.*

*04* *Enterprise IT will detect DDoS attacks directed at it but won't see malware related traffic or attacks on 3rd party servers.*

*05* *Infected devices will almost always communicate with malicious servers to download malware or exfiltrate data.*

*Case Studies* >

## 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.

## 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.)

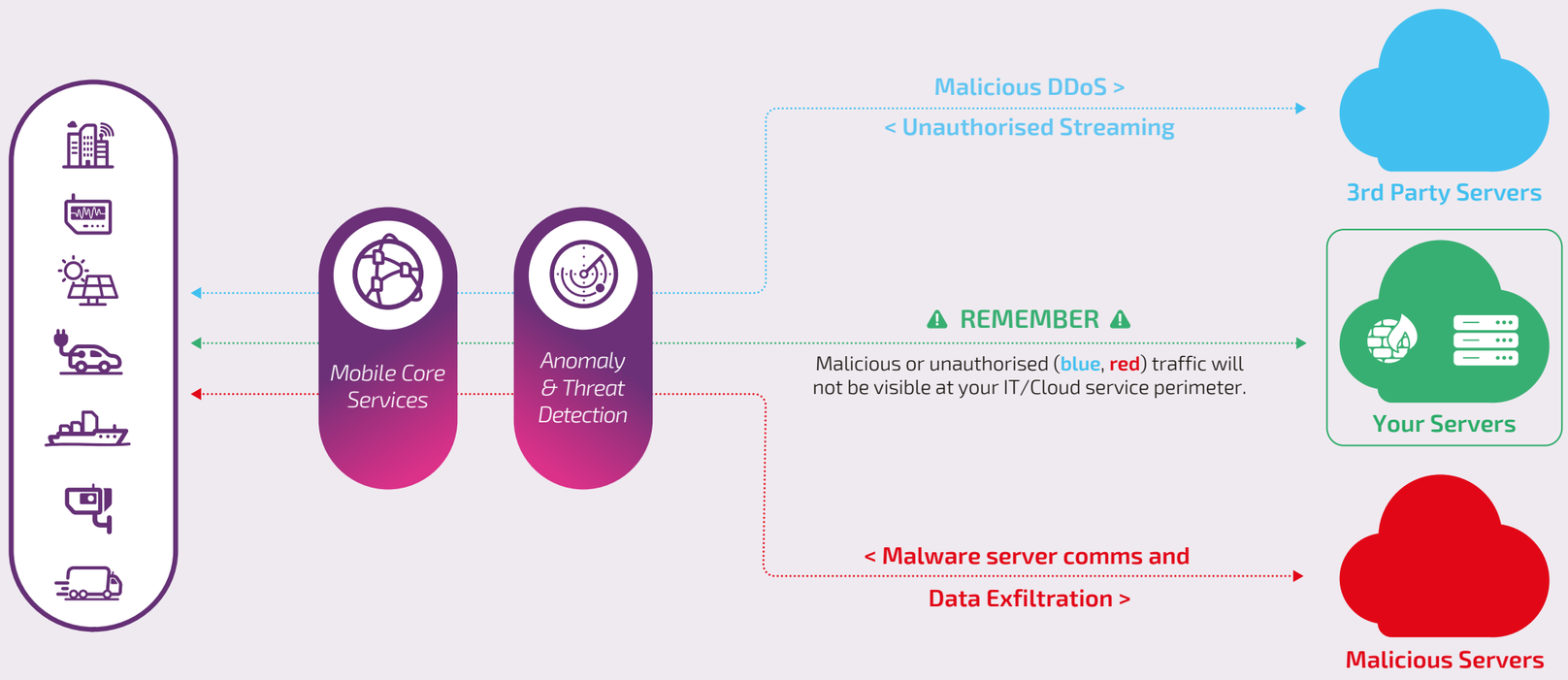
For IP backdoors, these methods detect unusual outbound connections or traffic to suspicious IPs that deviate from expected communication patterns of the device. Such backdoors may allow remote control or data exfiltration, both of which leave identifiable behavioural traces.

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.

**Figure 1:**

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




*What are the early warning signals?*

Service Levels and Benefits

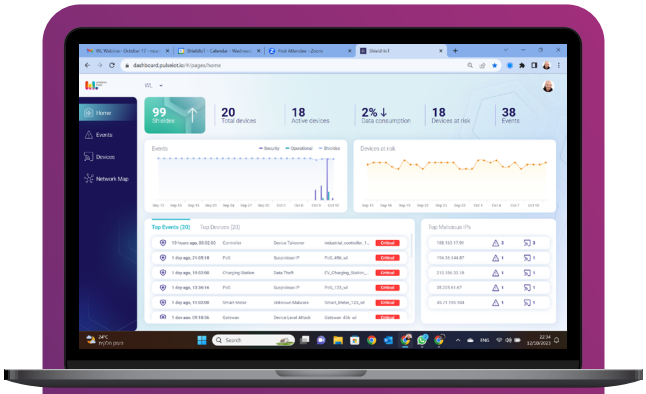
# The Early Warning Signals

**Our Anomaly & Threat Detection (ATD) solution delivers a pre-emptive cyber-security capability which monitors IoT device behaviour and traffic directly in the mobile core network.**

Powered by AI, it provides visibility and actionability for out-of-perimeter cellular IoT devices without any need for software agents on devices.

**ATD detects**

- Suspicious IPs
- Device backdoors
- Remote code execution
- Evidence of misconfigured devices
- Abnormal Port Connections
- Botnet detection
- Operational insights about ports and protocols



## How it works...

**The solution does not require any software agents to be installed on IoT devices and does not compromise your data privacy or system performance.**

Only packet headers from device-cloud communications are 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 a customer portal (UI) for investigation and remedial action.

**Service extensions are also available to support:**

- Automated response
- Threat prevention
- Regulation and Compliance

Service Levels and Benefits

## Monitoring and Detection

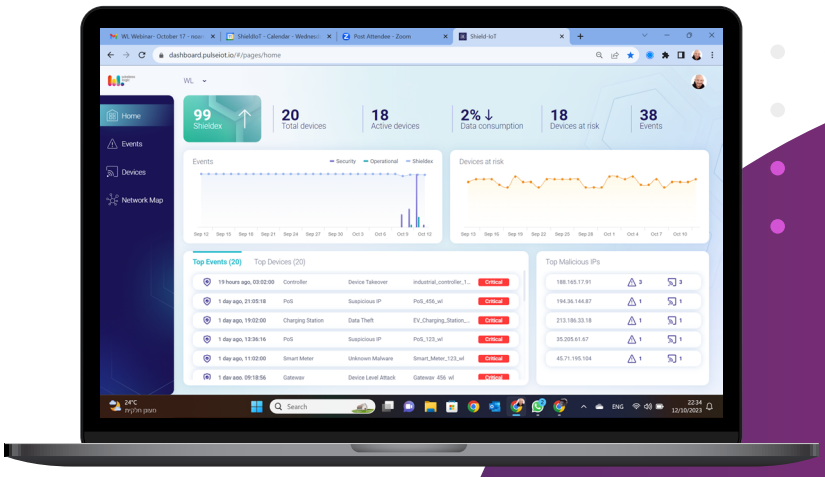
Receive real-time device intelligence and threat detection insights via the customer portal (UI).

## Response and Prevention

Upgrade to add Threat Management and Prevention capabilities. In addition to UI access, this includes export capabilities to management systems including Security Information and Event Management (SIEM), connectivity management platform (CMP), service desks (support ticketing), email.

## Regulation and Compliance

Upgrade to access features which help achieve compliance with Cybersecurity and Data Privacy regulations. This includes access to the Automated Compliance Report Generation Engine which provides evidence of continuous IoT network monitoring, responses to threats and evolution of security posture over time.




## Key Features

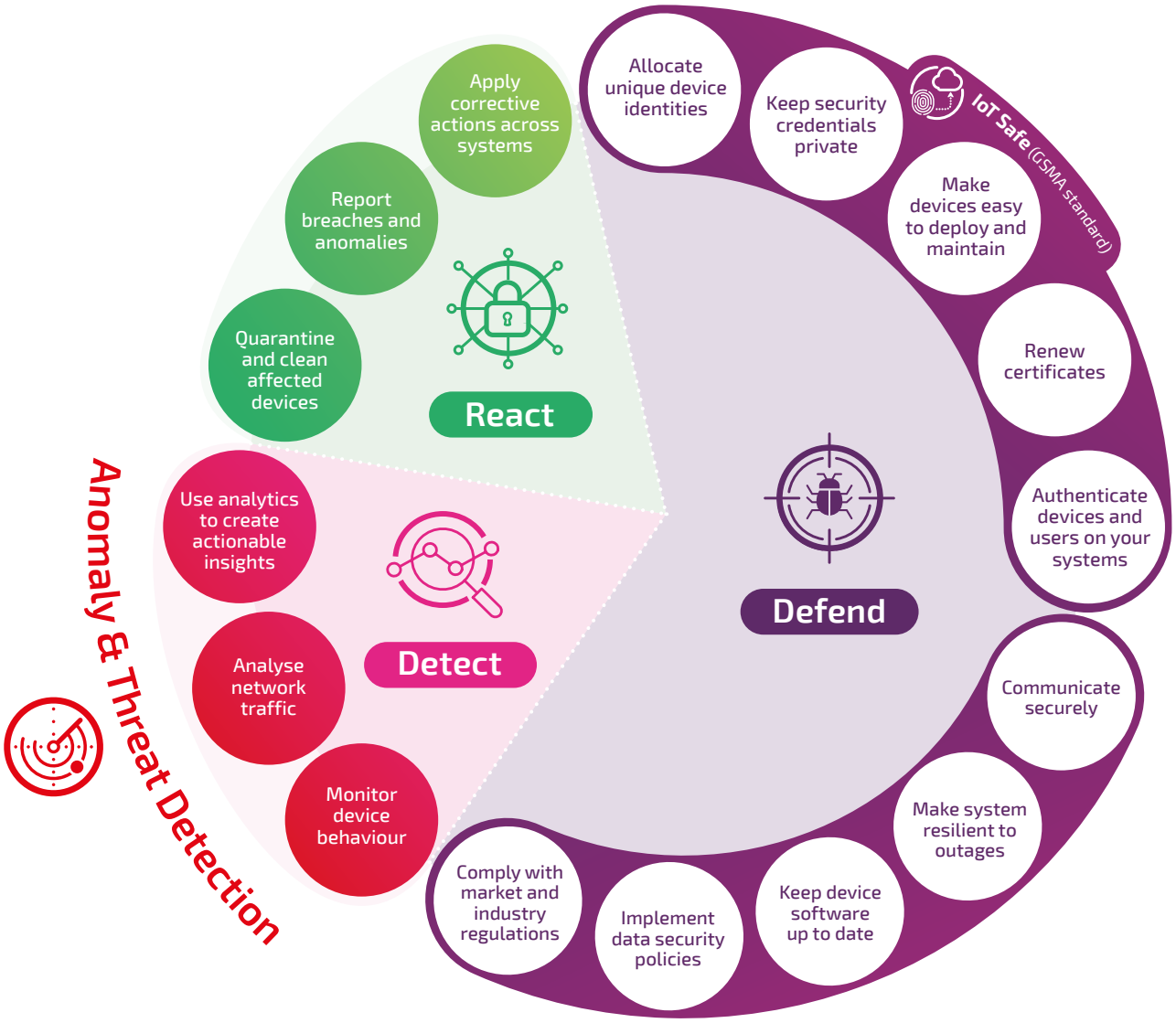
Asset Visibility | Actionable Device Alerts | Event Analysis | Network Maps | Multi-Tenant Support | Insights & Recommendations | API Integration | Compliance Reports

*Read more about our IoT Security Framework* ➤

# Wireless Logic **IoT Security Framework**

**IoT security is never ending, since new threats come up consistently and companies, even those who have already adopted best cybersecurity practices such as Anomaly & Threat Detection, need to take all levels of measures to keep their networks, devices, data and applications secure and protected.**

Our IoT Security experts have designed a framework which we use to help businesses assess their capacity for risk and build and implement a strategy to keep their reputation and revenue secure. It consists of 16 provisions which help enterprises Defend, Detect and React against IoT cyber-security threats.




**In this guide so far, we've covered Detect – our Anomaly Detection platform in detail.** There are technology solutions for many of the 16 provisions, but the framework also addresses people, processes and capacity for risk. The appropriate level of security might be dictated by your customers, by industry standards or by your assessment of acceptable risk and a trade-off between other factors such as price, compute resource or ease of use.

*The Wireless Logic IoT Security Stack...*

# 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.

*Contact us...*

**Wireless Logic has been a leader in the IoT connectivity sector for +20 years and has built this security framework using the experience and insights from hundreds of customer engagements.**

Contact us to learn how to apply the IoT security framework to your business.

## Contact us today...

to talk to an expert or book a free IoT Security Assessment
**wirelesslogic.com/iot-security-assessment**

Call: **+44 (0)330 056 3300** Email: **hello@wirelesslogic.com**
Web: **wirelesslogic.com/anomaly-detection**

wireless logic

UK_ID_C181023_V4_U160925