Anomaly Detection

IoT Device Intelligence and Threat Management

Anomaly 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 domain and in huge quantities. Until recently, this made them more susceptible to cyber-crime and more difficult to monitor and manage.

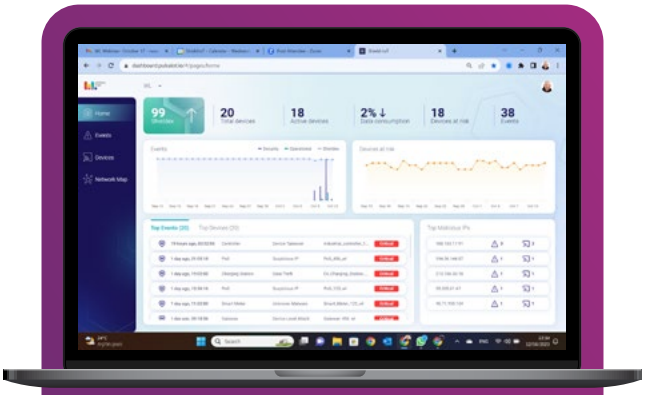
Anomaly Detection from Wireless Logic uses AI to constantly monitor IoT device communication patterns and enables Enterprises to detect early warning signals of operational or cyber-security issues across large IoT deployments. If left undetected, these issues can lead to chronic operational challenges, cyber-security breaches, loss of reputation and revenue or financial penalties in the form of regulatory fines.

The benefits of Anomaly Detection...

IoT Device Intelligence and Threat Management

Our Anomaly Detection platform identifies the first signs of unexpected IoT device communication issues caused by device malfunctions or cyber threats. The issues can present themselves in a number of different ways including...

- communication frequency changes
- zero data usage (devices are offline)
- abnormal downloads
- higher volume data transmissions
- communication with unusual server endpoints



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

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

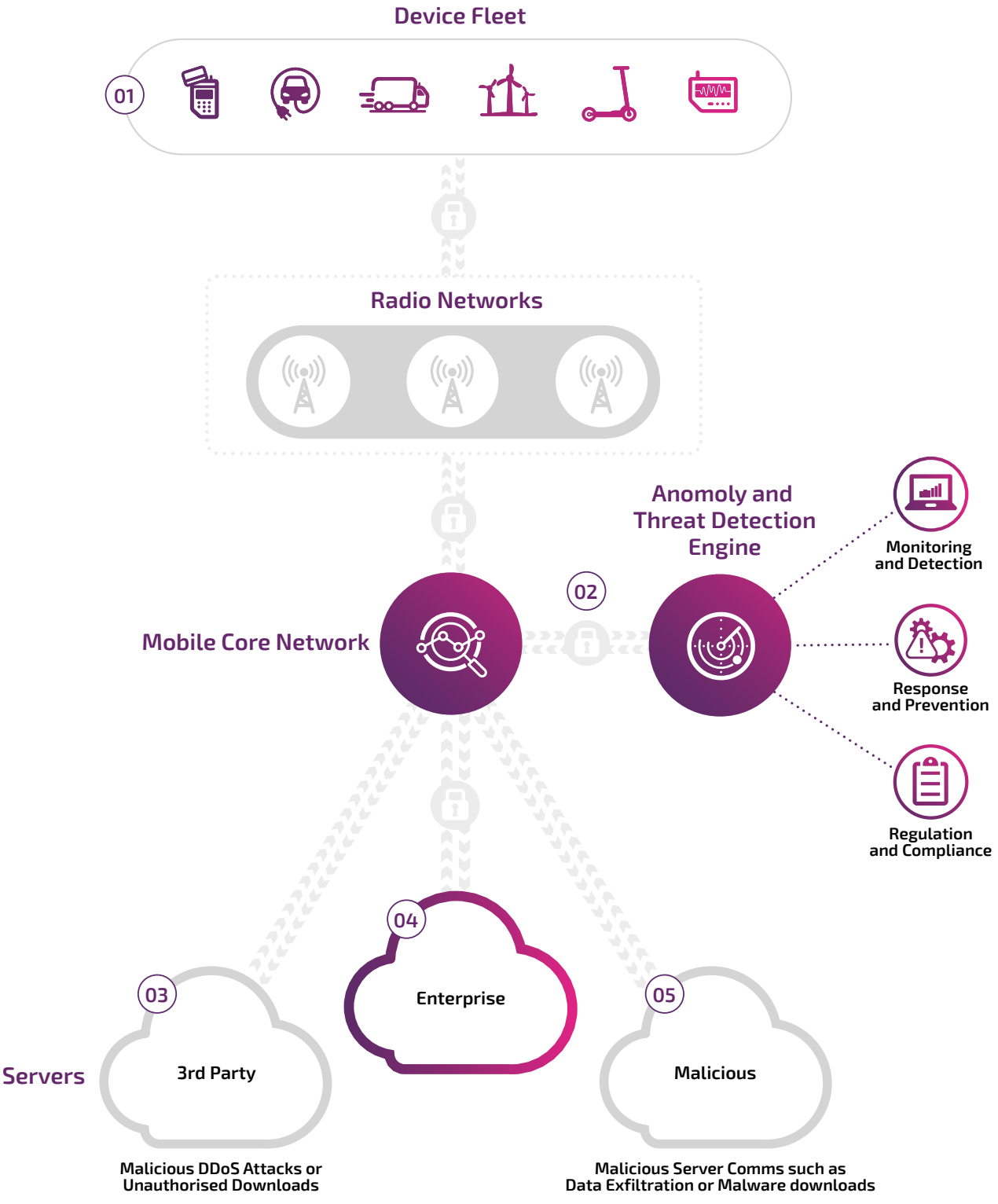
Breaches can lead to downtime as systems are investigated, cleaned, and restored. This can disrupt normal business operations, impacting productivity and revenue generation.

Regulatory Consequences

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

How Anomaly Detection works...

How Anomaly 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.*

Feature highlights...

Service Levels and Benefits

Monitoring and Detection

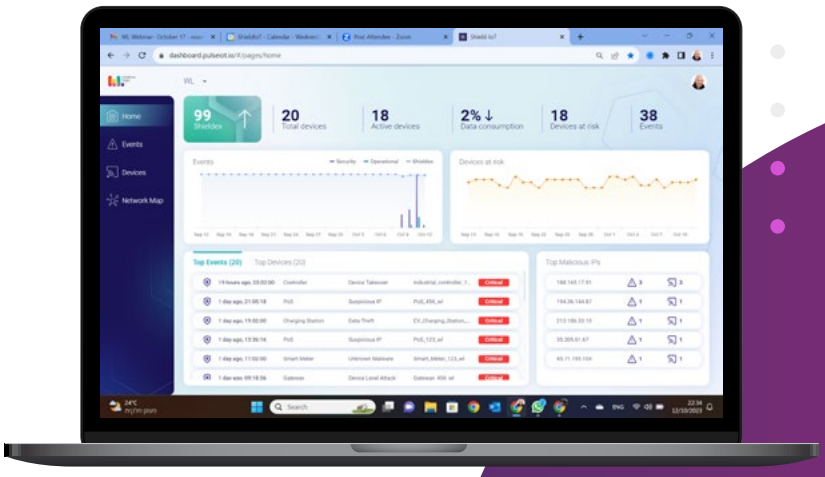
Receive real-time device intelligence and threat detection insights via the customer portal (UI).

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

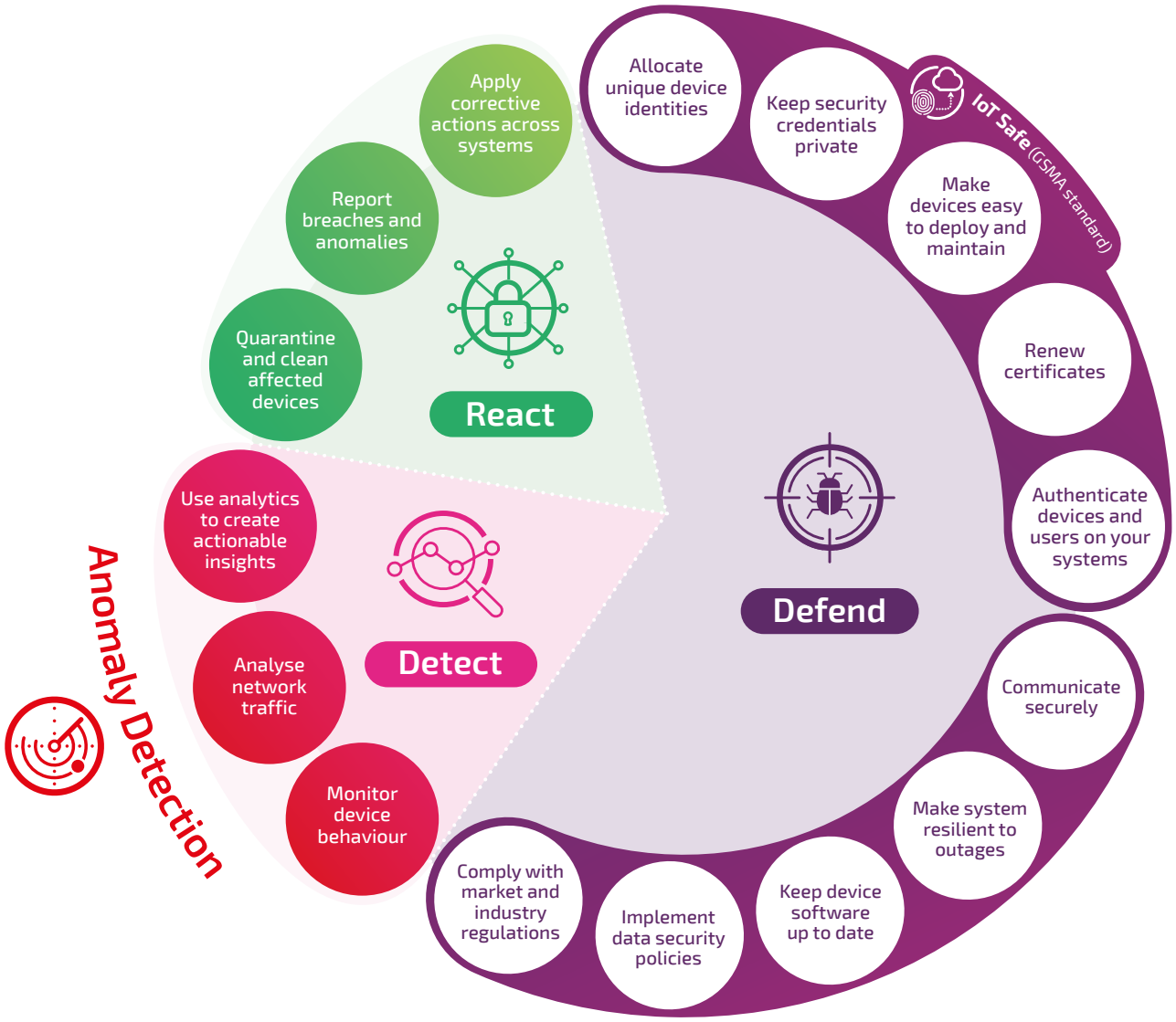
Asset Visibility | Actionable Device Alerts | Event Analysis | Network Maps | Multi-Tenant Support | Insights & Recommendations | API Integration | Compliance Reports

Read more about IoT security...

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 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**

24/7 Global Operations

Our global NOC/SOC service provides 24/7 monitoring, reporting and resolution of operational and security issues.

Application Development

Develop and model your application with security at the forefront of the design.

Anomaly Detection

Monitor device to cloud end-point communication and highlight deviations from normal behaviour.

Device Management

DevicePro enables solution providers, OEMs and Enterprises to monitor and remotely manage devices and hardware in real time.

Secure Private Networking

NetPro provides secure and resilient private networking which integrates Enterprises to their IoT devices and services.

Connectivity Management

SIMPro simplifies and automates connectivity management on a single secure platform with API or UI access.

Conexa

Our built for IoT mobile core network provides real time control and monitoring of IoT device behaviour.

Cloud Secure

Includes IoT SAFE technology to resolve IoT device identity challenges and enable secure dynamic scalability.

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/iot-solutions/iot-security**

wireless logic

UK_ID_C181023_V3_U130324