AI driven Anomaly Detection

Securing IoT devices from potential security threats is paramount, yet equally crucial is the ability to identify and address potential dangers. Without vigilant monitoring of IoT devices, applications and networks substantial harm could be inflicted before a breach is even detected. This is where Anomaly Detection plays a pivotal role.

Anomaly Detection is the process of identifying activity that deviates from the established norm. This could involve abnormally high or unusually frequent data transmission. It's important to note that anomalies may arise from malfunctions rather than hacks. Regardless of the cause, prompt awareness and action is crucial.

IoT devices often operate in unattended environments, rendering them susceptible to cyber crime. For hackers, these devices can serve as gateways into an enterprise systems for purposes like data theft or initiating a ransomware attack. Without insight into how they are operating, companies remain unaware of potential compromises. In the event of a breach, it's imperative to swiftly pinpoint and isolate it to prevent further harm.

While IoT security commences with safeguarding devices, networks, and systems, it's incomplete without the ability to detect and respond to anything out of the ordinary.

The benefits of Anomaly Detection...

The benefits...

Asset Intelligence

Anomaly Detection identifies the first signs of unknown cyber attacks, offering businesses protection against:

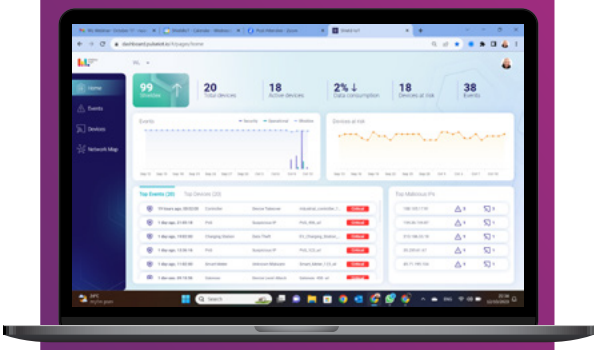
Financial Losses
Breaches cost money. There may be a need to investigate the cause, recover systems, install new security measures, pay fines or ransoms and seek expert assistance.

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.



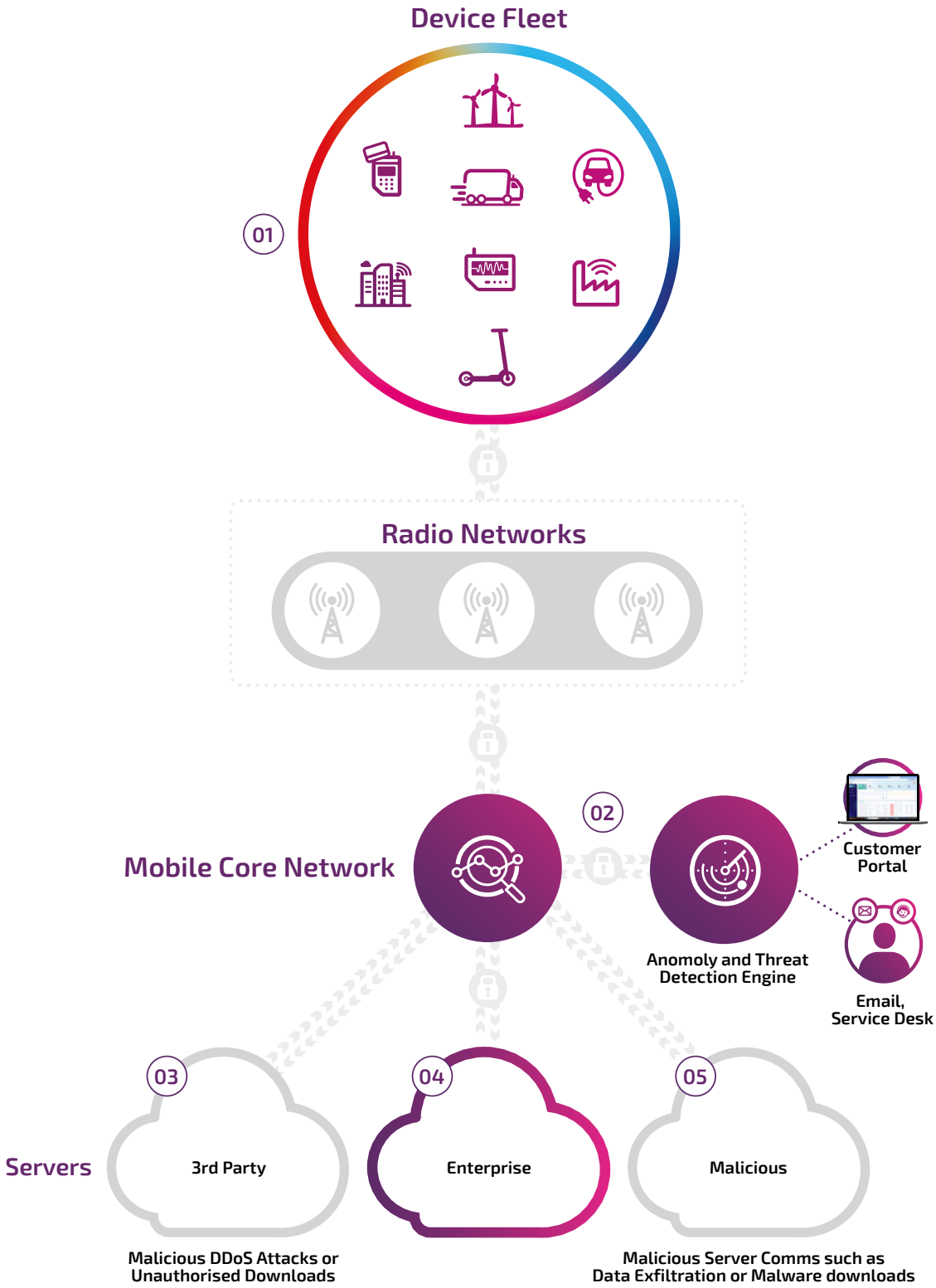
How it works...

Our Anomaly Detection platform analyses device-to-cloud network traffic statistics to detect the first signs of unknown cyber attacks and operational events.

The data is mirrored from our mobile core and detected threats are displayed on a multi-tenant dashboard. Threats are automatically mitigated by combining real-time actionable alerts with closed-loop prevention controls such as SIM barring, data throttling or downloading new firmware.

How Anomaly Detection works...

How Anomaly Detection works...



01 *Devices can be spoofed/hijacked and used to launch DDoS attacks on servers.*

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 *While the Enterprise Server will detect DDoS attacks launched against them, they wouldn't see malware related traffic or attacks on 3rd party servers.*

05 *Devices infected with malware will almost always communicate with servers to download malware or exfiltrate data.*

Feature highlights...

Feature highlights

- **Any device and application**
  Context-free detection, applicable to any IoT device or application, on any scale, anywhere in the world
- **Accurate detection**
  5 times more accurate in comparison to other solutions and reduces detection time from weeks/days to minutes/hours
- **Alerts & notifications**
  Generate actionable insights to enable automated threat prevention and investigation
- **Agentless**
  AI driven Anomaly Detection combines threat intelligence and rule based detection engines
- **Realtime**
  Full visibility of IoT estate, including asset risk, network behaviour, attributes and usage trends
- **Privacy compliance**
  Analyse encryption-free metadata to comply with industry regulations.

Context free detection...

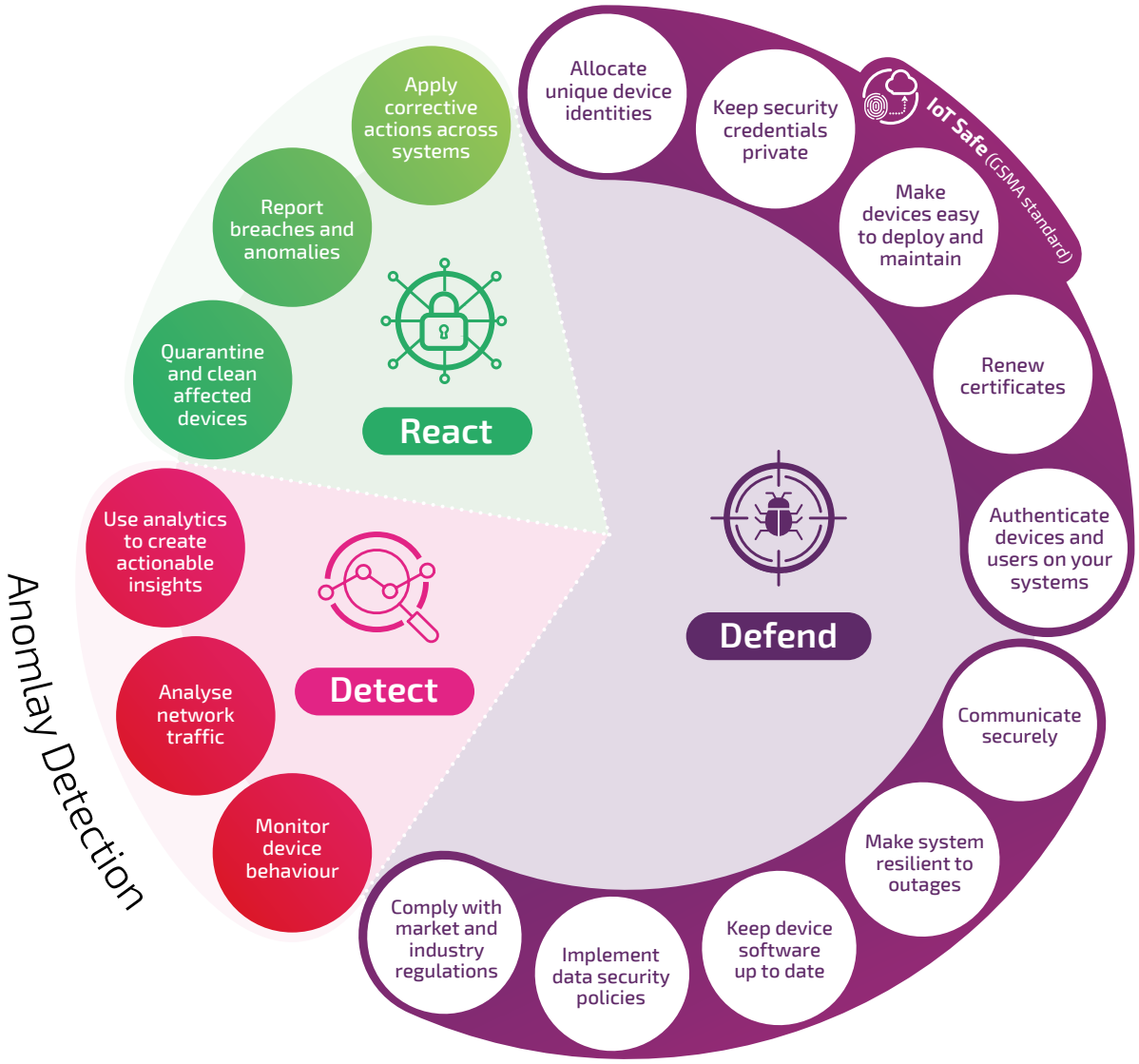
Applicable to any IoT device or application, on any scale, anywhere in the world

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

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

IoThink Solutions

Model and optimise your solution at start of the design process.

Anomaly Detection

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

DevicePro

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

NetPro

Secure and resilient private networking which integrates. Enterprises with their Cellular IoT device fleets.

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: **0330 056 3300** Email: **hello@wirelesslogic.com**
Web: **wirelesslogic.com/iot-solutions/iot-security**

wireless logic