



# Security Management Framework

**The constantly evolving IoT security threat landscape means that even enterprises who have already adopted best practices need to maintain both defensive and active measures to mitigate risks across their IoT device fleet, communication networks, data and application layers.**

The number and type of cyberattacks - ransomware, malware, device spoofing, man-in-the-middle - against IoT systems are steadily rising and businesses need to protect themselves against safety, operational, financial and reputational issues which can arise from security breaches.

The Wireless Logic IoT Security Framework provides enterprises with a 360-degree view of IoT security and a range of Defend, Detect and React measures covering processes, people, legislation, regulatory compliance and technology solutions including advanced SIM, private networking and security AI.



*Find out more about the Security Management Framework... >*



### 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.

Why product connectivity, security and compliance life-cycle management must not be an afterthought.

#### > 1.5 Billion

*The number of attacks on IoT devices in 1H 2021 alone (detected by Kaspersky)*

#### > 85%

*of businesses say security concerns are a major barrier to adopting connected devices (Omdia)*

#### > 77%

*Increase in malware attacks on IoT devices in H1/2022 (Sonicwall)*

#### > \$4.5M

*Average cost of a ransomware attack (IBM)*

#### > \$3M

*Average cost savings associated with fully deployed security AI and automation (IBM)*

#### > \$600M

*A single medical device recall due to an unaddressed vulnerability can cost up to \$600M (McKinsey)*





**IoT cyber-security legislation is increasing in scope and application with some quite significant laws now introduced in the US, EU and UK.**

- Cyber Resilience Act (EU)
- IoT Cybersecurity Improvement Act (USA)
- Product Security and Telecommunications Infrastructure Bill (UK)

It's critical to keep on top of the changes. The focus of regulation, until very recently, has been on providing voluntary guidelines for device manufacturers, but the coverage is expanding and the guidelines are evolving into concrete obligations in many cases. These are mostly consumer-oriented and not immediately applicable to B2B IoT, but they will become established best practice for any IoT deployment. Enterprises can and should be looking for vendors that are compliant with the critical parts of these regulations.



**conexa**  
the network for things

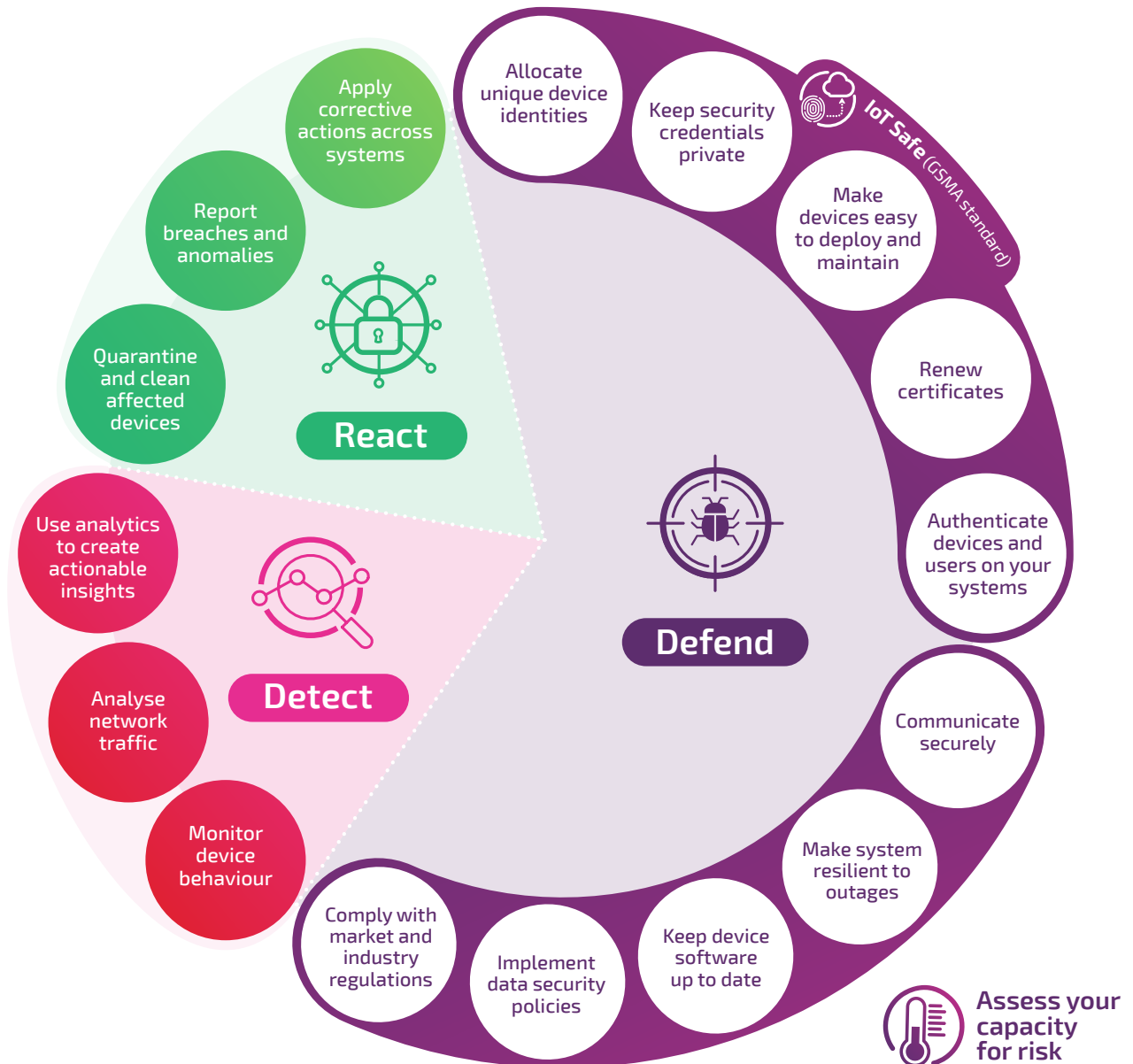
**Act now.** IoT solutions which align with upcoming legislation and standards will be differentiated in enterprise procurement processes.




# 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 and 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.



**This 360 degree security framework helps customers protect their investments, their reputation and revenue.**

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

There are technology solutions for many of the 16 provisions but the framework also addresses **people, processes,** and attitude or **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.

Read on for the next level of insight behind each of the framework provisions and for a view of where and how Wireless Logic security stack can help.



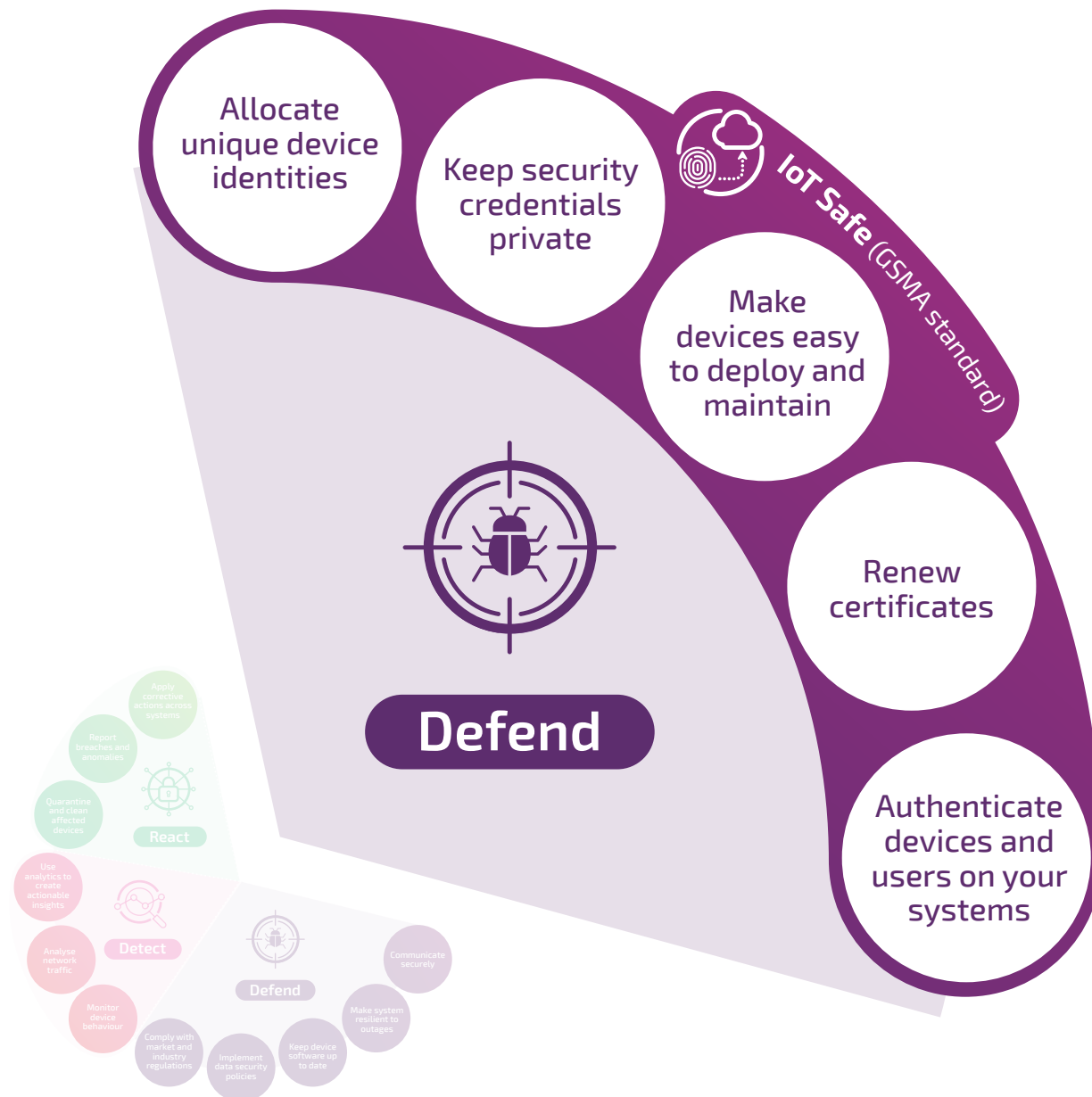
Wireless Logic has been a leader in the IoT connectivity business for +20 years and have built this security framework using the experience and insights from hundreds of thousands of customer engagements.



# 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



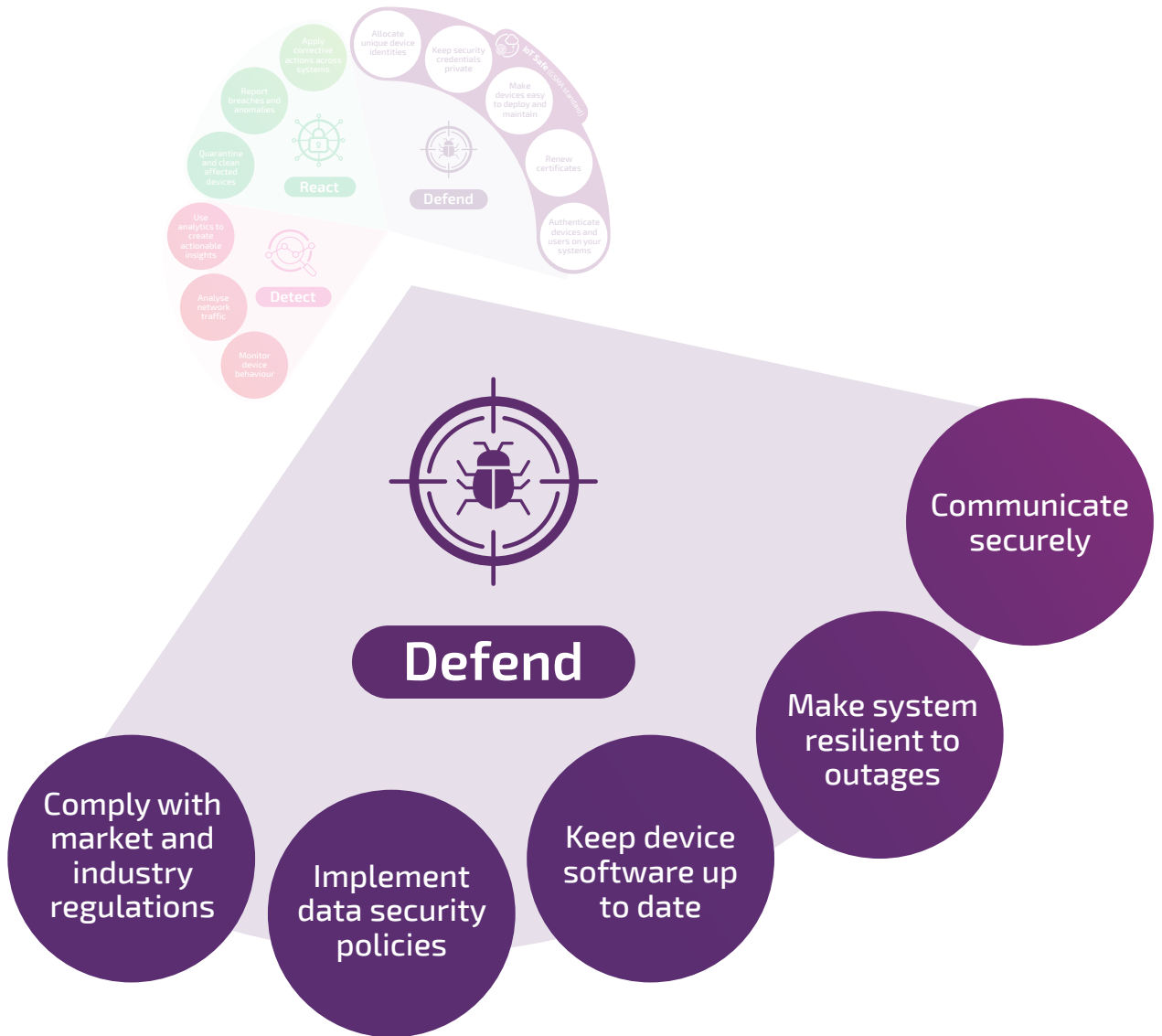




Part 2

# Defend against cyber threats

- system resilience, people and processes



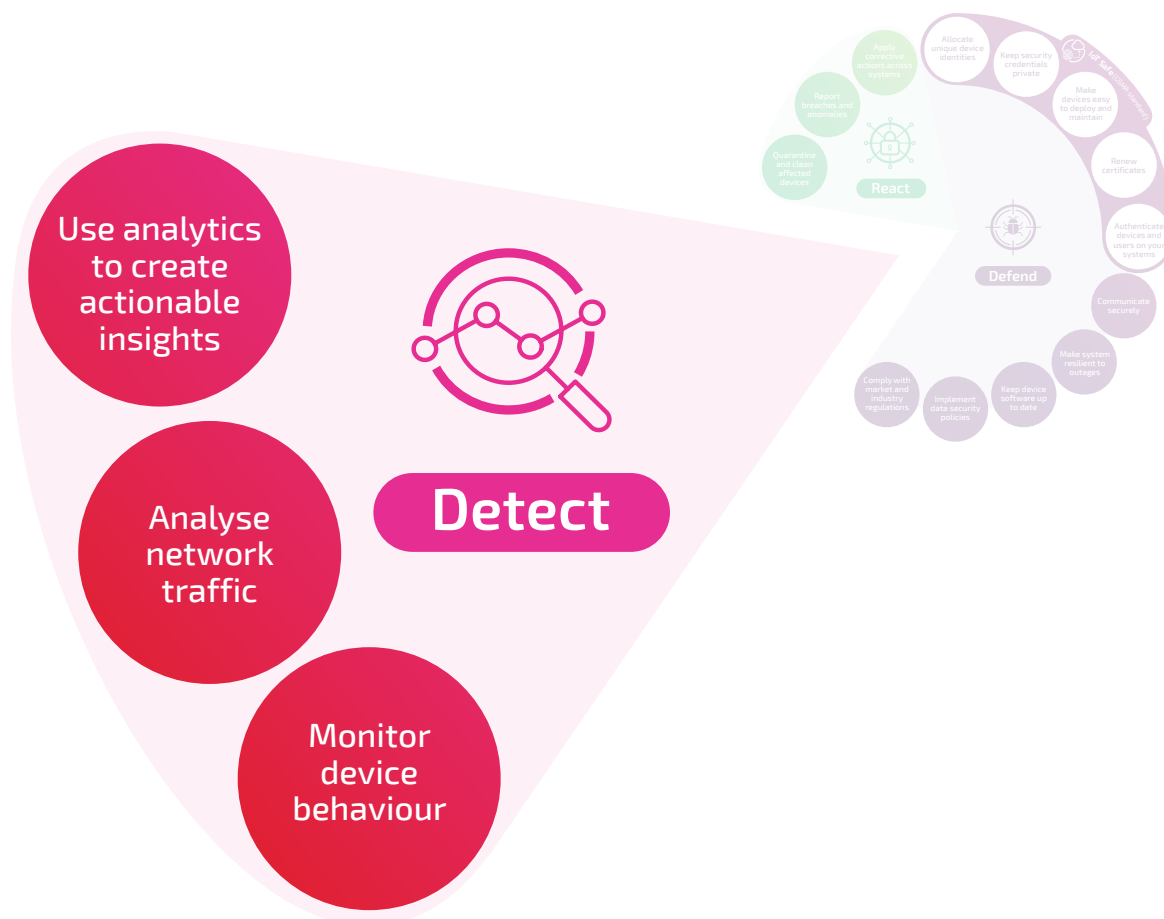
## The non-negotiables:

- Insist on 99.99% availability
- Redundant/Resilient VPN Infrastructure
- People, Processes and Partners - these are your biggest security risk
- Choose partners with a strong reputation and security credentials





## Detect threats using security AI that flags device and network anomalies



### How does real-time anomaly detection work?

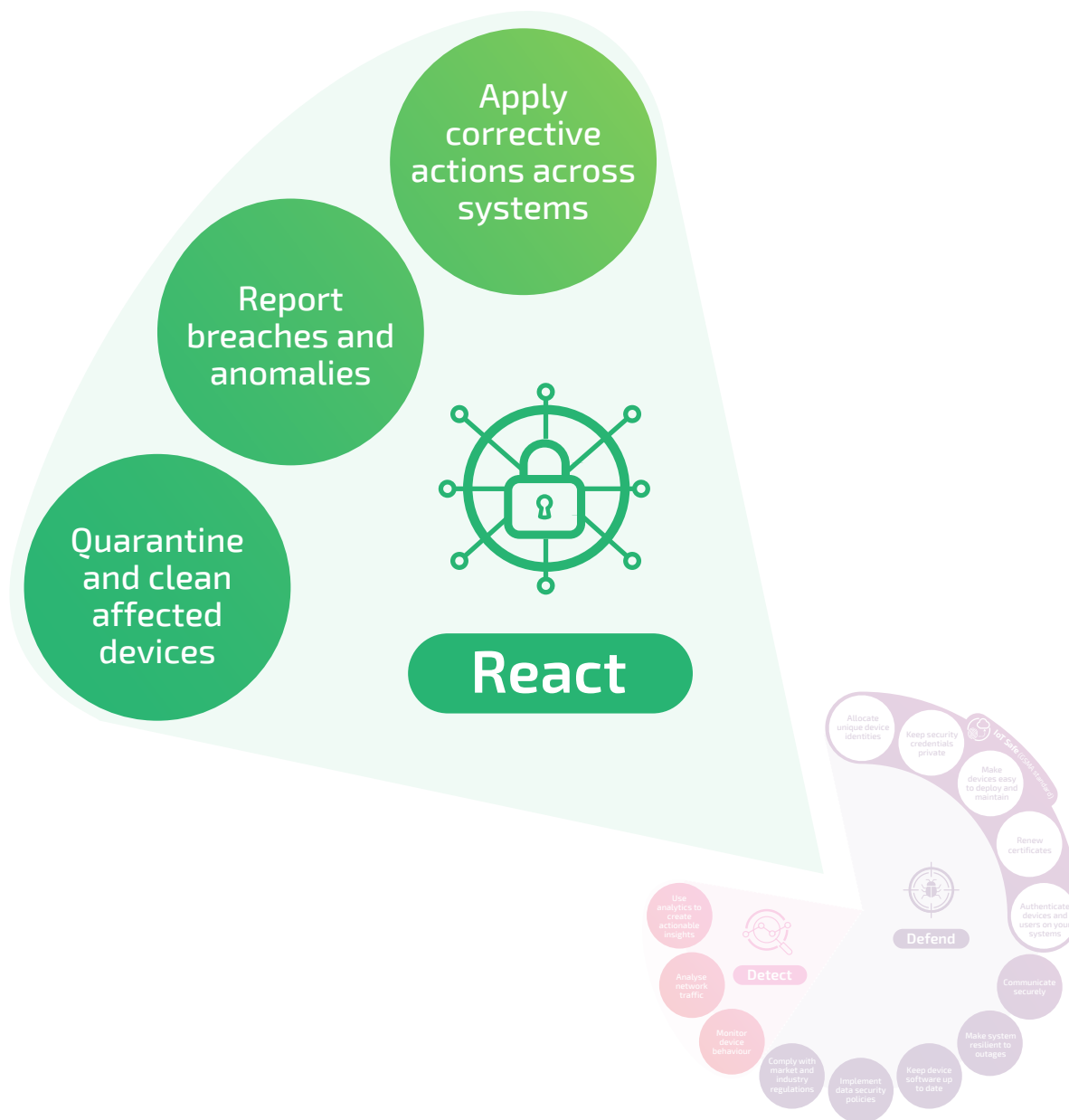


- Profile your IoT network baseline behaviour
- Monitor device, network traffic and application level behaviour
- Real-time Alerts and Automate responses
- Single device or fleet, system-wide





**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**



## **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.

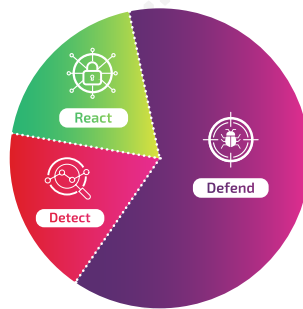


# Mapping **our security stack** to a device - network-cloud hierarchy

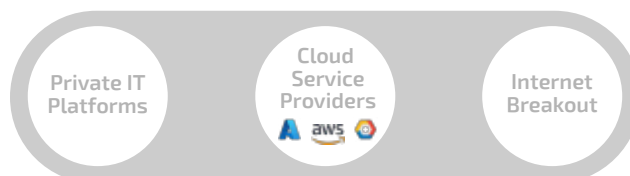
## Things we connect...



## How...



## Cloud and Enterprise Interconnects





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



---

## Contact us today...

to talk to an expert or learn how to  
apply the IoT Security Framework  
to your business

Call: **0330 056 3300**

Email: **hello@wirelesslogic.com**

Web: **wirelesslogic.com**

---