WIRELESS LOGIC **IOT CONNECTIVITY**

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...

Why use a 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 and standards... ➤

Legislation and Standards

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**

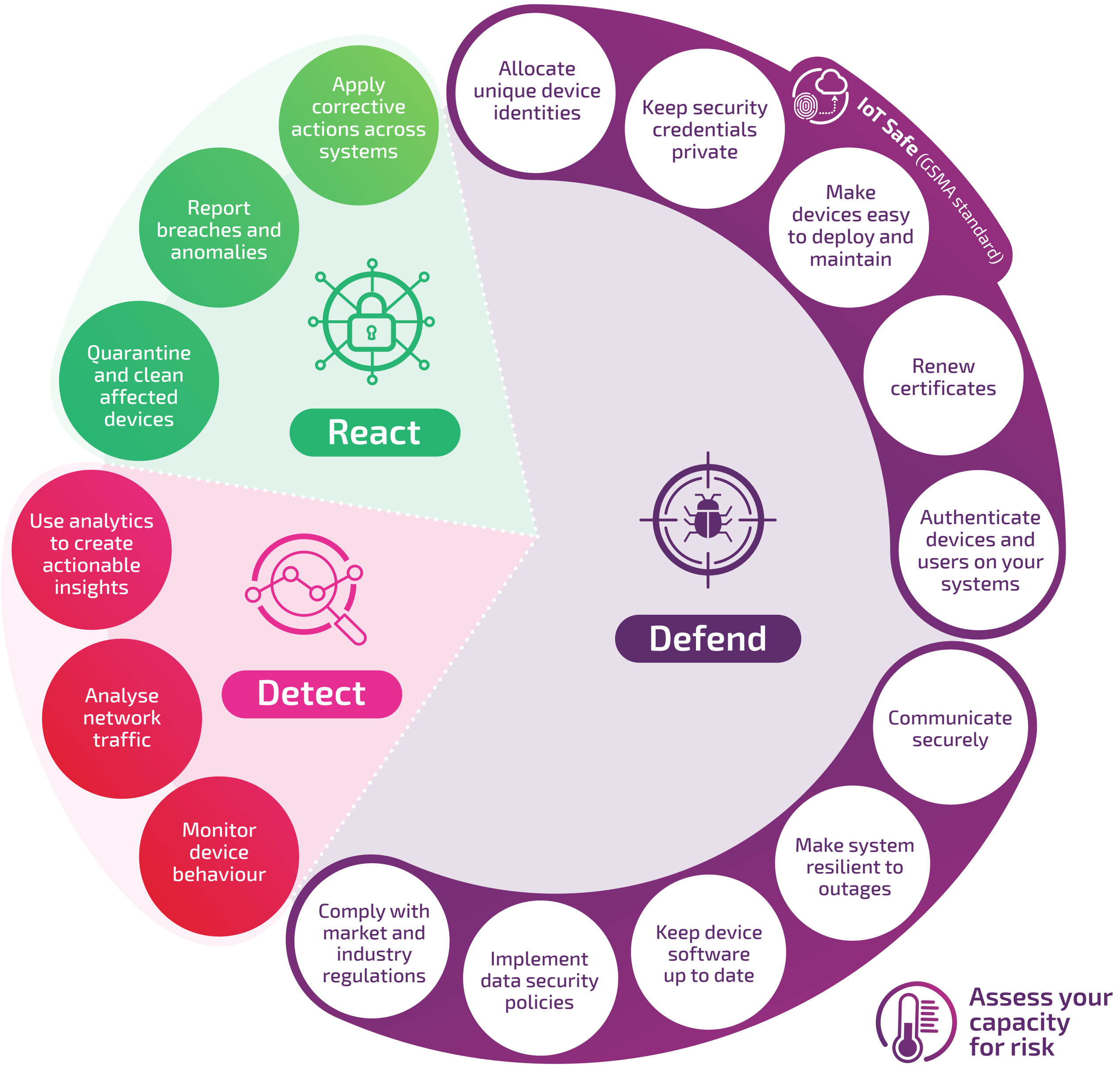
Act now. IoT solutions which align with upcoming legislation and standards will be differentiated in enterprise procurement processes.

Introducing the IoT Security Framework...

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.


Apply corrective actions across systems
Report breaches and anomalies
Quarantine and clean affected devices
React
Use analytics to create actionable insights
Analyse network traffic
Monitor device behaviour
Detect
Allocate unique device identities
Keep security credentials private
IoT Safe (GSMA standard)
Make devices easy to deploy and maintain
Renew certificates
Authenticate devices and users on your systems
Defend
Communicate securely
Make system resilient to outages
Keep device software up to date
Implement data security policies
Comply with market and industry regulations
Assess your capacity for risk

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.

About the framework... ▶

A 360 degree framework

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.

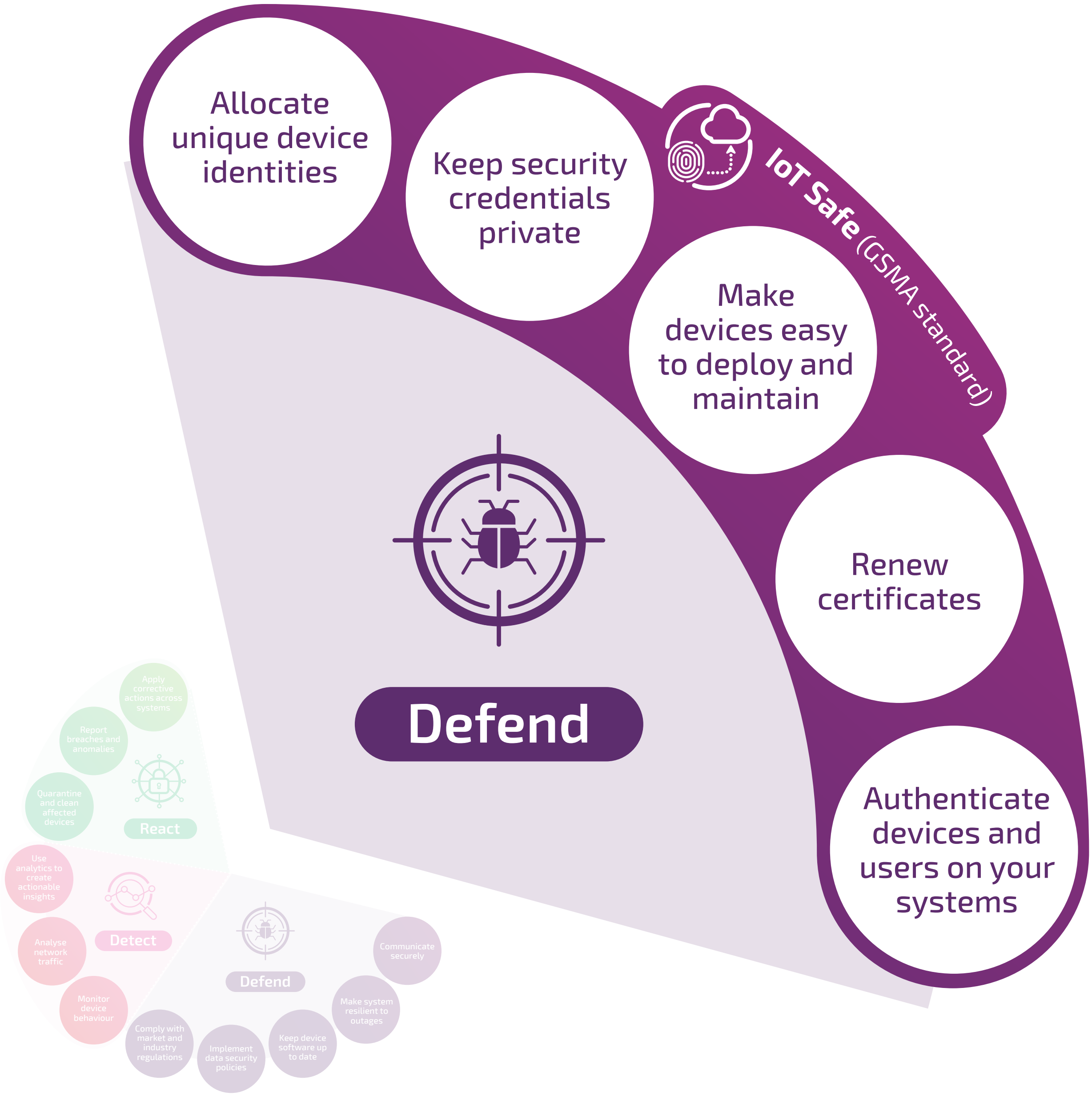
Wireless Logic has been a leader in the IoT connectivity business for +20 years and have built this security framework using the experience and insights from hundreds of thousands of customer engagements.

Manage Identity...

Part 1

Defend against cyber threats

- manage identity



Allocate unique device identities

Keep security credentials private

Make devices easy to deploy and maintain

Renew certificates

Authenticate devices and users on your systems

IoT Safe (GSMA standard)

Defend

Apply corrective actions across systems

Report breaches and anomalies

Quarantine and clean affected devices

React

Use analytics to create actionable insights

Analyse network traffic

Monitor device behaviour

Detect

Defend

Communicate securely

Make system resilient to outages

Keep device software up to date

Implement data security policies

Comply with market and industry regulations

End-to-end authentication with IoT Safe?

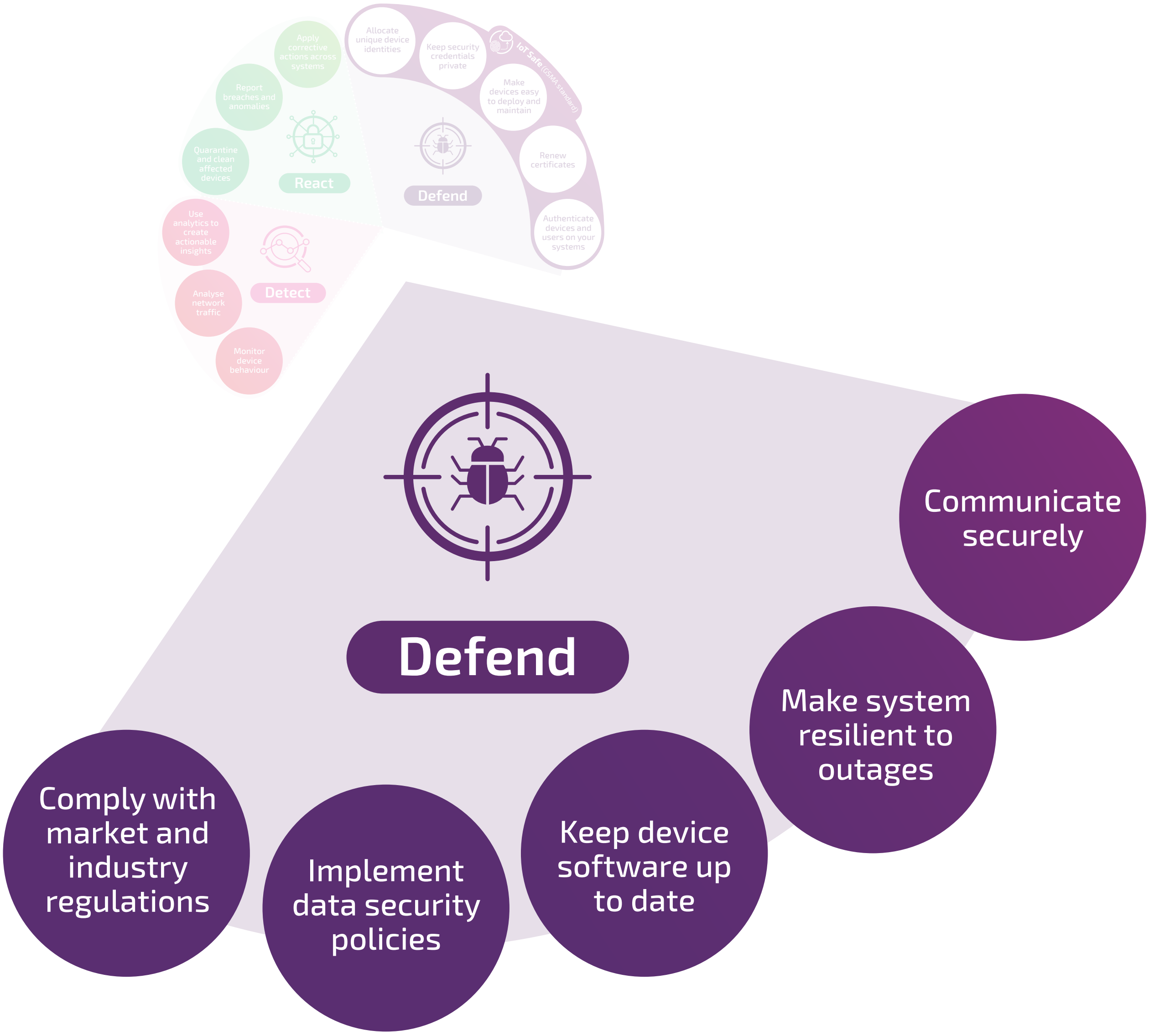
- Zero Touch Provisioning: wake up, connect, authenticate, communicate
- Remove security hardware overhead in your devices
- Cloud Portability. Lower cost certificate provisioning
- Reduced security complexity
- Evolve your security approach over time as new products are launched and threat

System resilience, people and processes... ▶

Part 2

Defend against cyber threats

- system resilience, people and processes

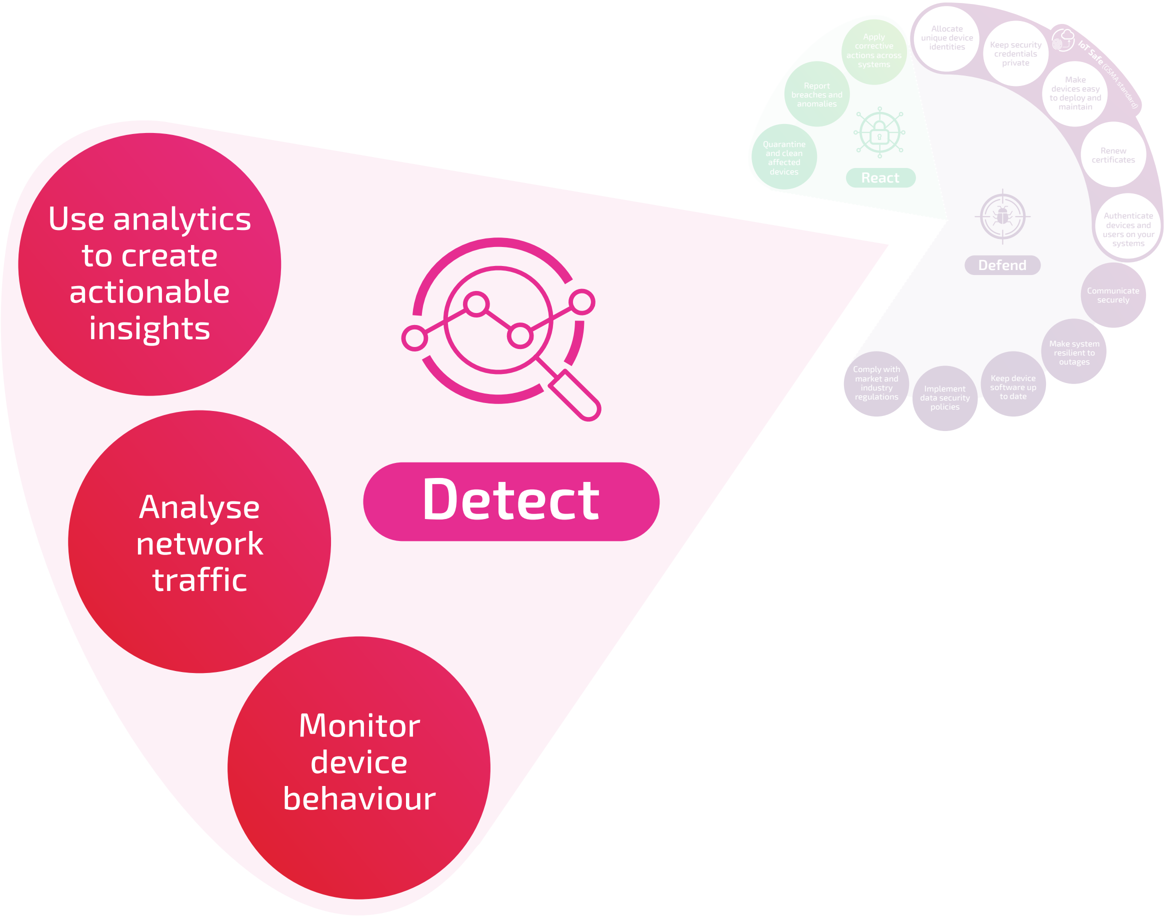

Apply corrective actions across systems
Report breaches and anomalies
Quarantine and clean affected devices
React
Allocate unique device identities
Keep security credentials private
IoT Safe (GSMA standard)
Make devices easy to deploy and maintain
Renew certificates
Authenticate devices and users on your systems
Defend
Use analytics to create actionable insights
Analyse network traffic
Monitor device behaviour
Detect
Defend
Communicate securely
Make system resilient to outages
Keep device software up to date
Implement data security policies
Comply with market and industry regulations

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...

Detect threats using security AI that flags device and network anomalies



Use analytics to create actionable insights

Analyse network traffic

Monitor device behaviour

Detect

React

Quarantine and clean affected devices

Report breaches and anomalies

Apply corrective actions across systems

Defend

Allocate unique device identities

Keep security credentials private

IoT Safe (GSMA standard)

Make devices easy to deploy and maintain

Renew certificates

Authenticate devices and users on your systems

Communicate securely

Make system resilient to outages

Keep device software up to date

Implement data security policies

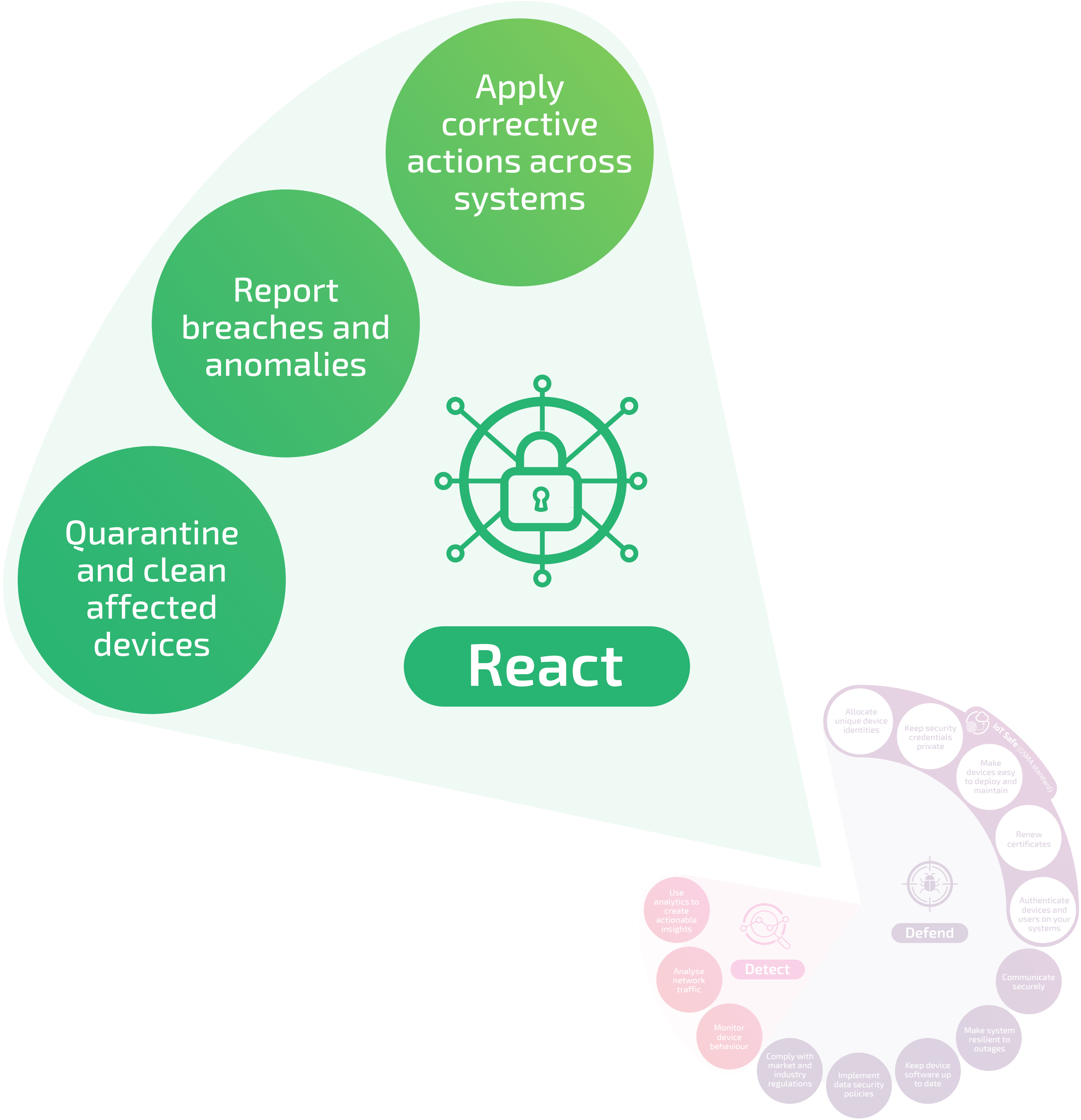
Comply with market and industry regulations

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...

React quickly to isolate security breaches and take remedial action.


Apply corrective actions across systems
Report breaches and anomalies
Quarantine and clean affected devices
React
Allocate unique device identities
Keep security credentials private
IoT Safe (GSMA standard)
Make devices easy to deploy and maintain
Renew certificates
Authenticate devices and users on your systems
Defend
Use analytics to create actionable insights
Detect
Analyse network traffic
Communicate securely
Monitor device behaviour
Make system resilient to outages
Comply with market and industry regulations
Implement data security policies
Keep device software up to date

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... ▶

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

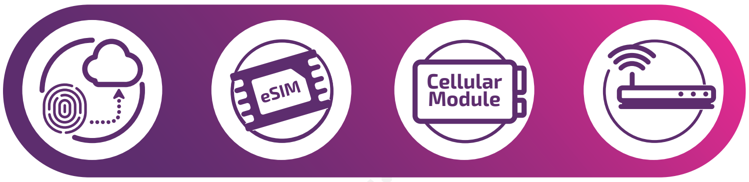
includes IoT SAFE technology to resolve IoT device identity challenges and enable secure dynamic scalability.

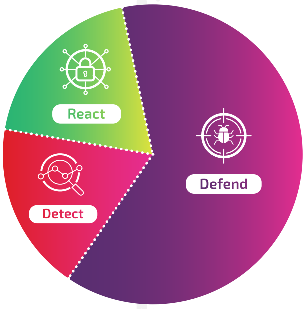
Mapping our IoT Security Stack... ▶

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

Things we connect...

How...





ioThink® Solutions

conexa
the network for **things**

Anomoly Detection

Cloud Secure

SIMPro

NetPro

DevicePro

Cloud and Enterprise Interconnects

Private IT Platforms

Cloud Service Providers

Internet Breakout

Get in touch to discuss how the Security Management Framework can be applied in your business ...

wireless logic

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**