Vodafone IoT:
Security by design strategy for IoT security

vodafone IoT

beecham research

Shaping the IoT future

Introduction

With the world becoming increasingly digitised, companies must continue to adapt, innovate, and expand their technological horizons to stay ahead. However, anything that is connected in today's world is at potential risk, and IoT is no different.

While the risks associated with insecure IoT deployments are real, they can be managed. With the right infrastructure, controls, and expertise, IoT can be deployed at scale with enterprise-grade security.

As an operator of critical national infrastructure, a pioneer in IoT technology, and collaborative leader involved in the development of security standards, Vodafone is at the centre of this development and through a multi-layered security model provides organisations with a trusted and secure foundation for global IoT success.

The Challenge of Security in an increasingly Connected World

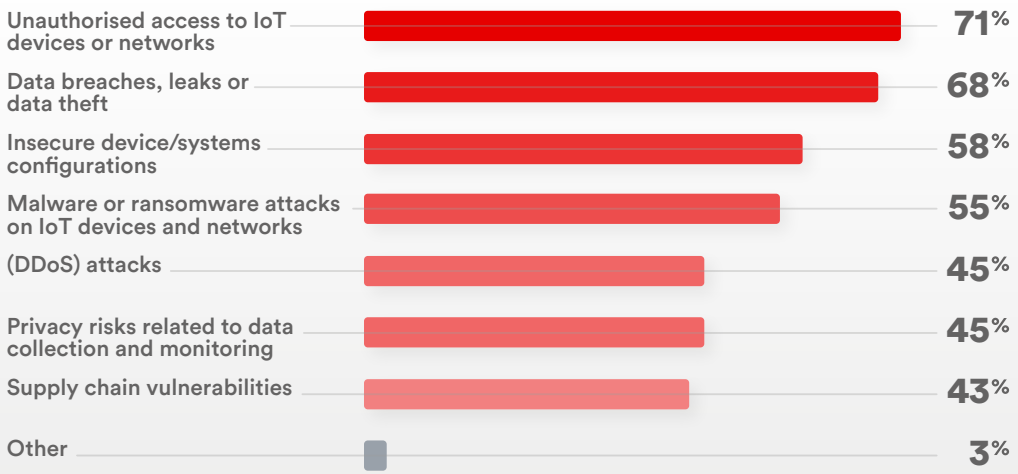
Connected technology is essential for businesses to stay competitive and innovative.

However, this interconnectedness comes with risks, as every connected device or system can potentially open a door to threat actors. Vulnerabilities in connected systems, whether caused by poor security practices or outdated software, can potentially become entry points for attacks, especially with the number of active IoT devices projected to soar to around 30 billion by 2030.

In Beecham Research's 2025 IoT security report, the top cited consideration for businesses using IoT was unauthorised access to devices or networks, with more than seven in ten respondents selecting this option – see **Figure 1**. This risk is not hypothetical, millions of IoT devices from companies all over the world have been compromised in recent years and used to launch attacks including coordinated botnet assaults against online content services.

On the other hand, as the array of challenges, vulnerabilities, and attack methods have evolved, so too have the defences of security teams.

Figure 1. The most relevant IoT security risks across industries.



Source: Beecham Research, Locking in Value with IoT Security, 2025

Key Features of an IoT Security Strategy

IoT-Specific Security

IoT solutions are composed of several different parts, each requiring individual resilience whilst seamlessly integrating with the rest. Where a weak link exists, there is an opportunity for threat actors to enter.

The variety and interconnectedness of IoT solutions demands specialist expertise. Choosing providers with knowledge and expertise in IoT-specific security is essential for the integrity of the whole system.

End-to-End Protection

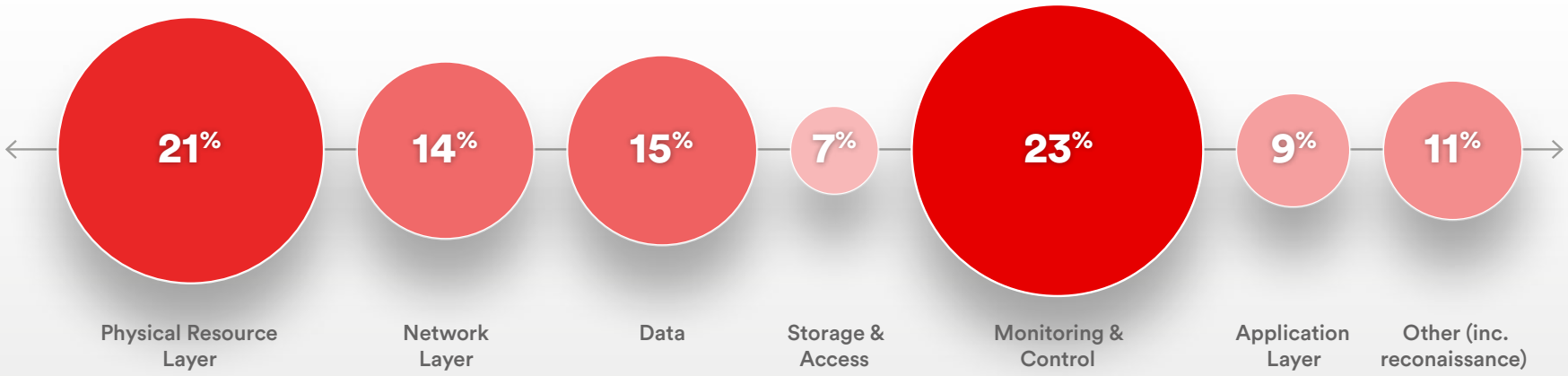
End-to-end security is vital for IoT because every link in the chain is at potential risk of an attack. Without comprehensive protection, vulnerabilities can be exploited, compromising the whole system. Moreover, the connections between each layer of the IoT stack can offer vulnerabilities to threat actors if security is not robustly deployed.

An evaluation of the attacks on smart factories by Sectrio (see **Figure 2**) demonstrated that, despite a slight skew towards the physical resource (device) and monitoring and control layers, all elements of the IoT stack can be targeted and must be defended.

An end-to-end security strategy is essential to protect the overall solution.

Protecting all the elements of a solution can be particularly challenging when the solution is built from a patchwork of suppliers, each managing their own elements.

Figure 2. Proportion of attacks targeted at each layer of the IoT solution in Smart Factories



Source: Sectrio, The Global OT and IoT Threat Assessment and Analysis Report 2024.

Security by Design

Security by Design aims to make sure that security is embedded into systems, applications, and devices from the outset, rather than being added retrospectively.

In terms of IoT, it is particularly important because of the unique security challenges the IoT ecosystem presents. Historically, many IoT devices were simple sensors and did not have the capacity to enforce strong security measures, nor enable patching post-deployment.

This is now evolving, with security becoming an integral part of every stage of IoT development, as part of a proactive approach to IoT security.

The Cellular Advantage

The common denominator of all IoT devices is their connection. This connection is what enables remote access – and with it, the potential for compromise. Securing the communication channel is therefore a critical step towards protecting the entire system.

Licensed cellular technology has a clear security advantage. Whereas many IoT devices and solutions will use the internet as a communication channel, the devices connected by a Vodafone IoT cellular enabled solution do not. They are linked over the (private) radio network to the nearest cell tower, then though private mobile "backhaul" to the Vodafone mobile data connectivity infrastructure (SGSN, GGSN etc), then via a Vodafone private fixed line connectivity product such as an IPVPN directly to the customer's IoT Application Server.

This is an extremely powerful control as device connectivity can be fully designed, for example we usually recommend that device-device communications are blocked and that devices are only allowed access to selected servers/IPs. Thus, the attack surface and attack vectors are massively decreased. This is controlled at the device end via connecting to a private APN (Access Point Name) that is dedicated to that customer/environment and controlled by the Vodafone mobile core infrastructure. Devices cannot be connected to and attacked from arbitrary entities on the internet.

Telecom operators are highly experienced in defending against cyber threats, as they face attempted breaches on a constant basis. This high level of activity demands advanced security operations that can detect, analyse, and shut down vulnerabilities before they can be exploited. Recognising the scale and importance of this challenge, Vodafone has invested heavily in global cyber security capabilities.

Figure 3. Key Principles of Security by Design in IoT.

Source: Beecham Research, Locking in Value with IoT Security, 2025.

Vodafone global, enterprise-grade security

Vodafone IoT currently supports and services a market-leading 200 million cellular IoT connections worldwide. With business operations, relationships, and partnerships in over 180 countries, Vodafone IoT is trusted by enterprises across many critical industries including healthcare, automotive, utilities, energy, emergency services, and has been recognised as a leader in the Gartner® Magic Quadrant™ for Managed IoT Connectivity Services for 11 years.

A Strategic Approach to IoT Security

Vodafone adopts a proactive, multi-faceted approach to security that aligns with its mission to promote trust and innovation.

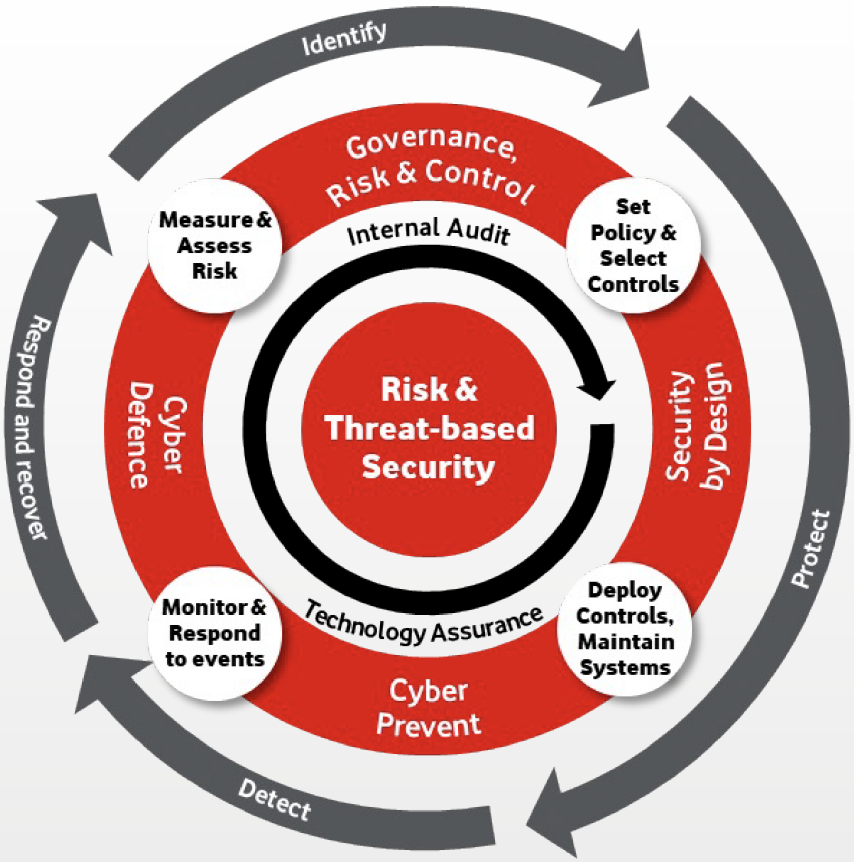
Our operating model and strategy responds to the challenging cyber threat landscape. We implement controls that are designed to prevent, detect, respond and recover from attacks. By taking this approach, we aim to minimise impact to customers and the services we provide.

We have implemented a globally consistent cyber security operating model that is based on the leading industry security standards published by the US National Institute of Standards and Technology ('NIST'). The model is designed to reduce risk by constantly identifying threats, protecting, defending and improving our security.

Our scale means we benefit from global collaboration, technology sharing and deep expertise, and ultimately have greater visibility of emerging threats. We augment our internal capabilities where necessary with third party specialist technical expertise.

Vodafone acts as the sole service owner – reducing fragmentation, simplifying compliance, and closing operational gaps. By operating as a managed service, Vodafone IoT encompasses all aspects of the solution.

Figure 4. Vodafone's Cyber Security Operating Model



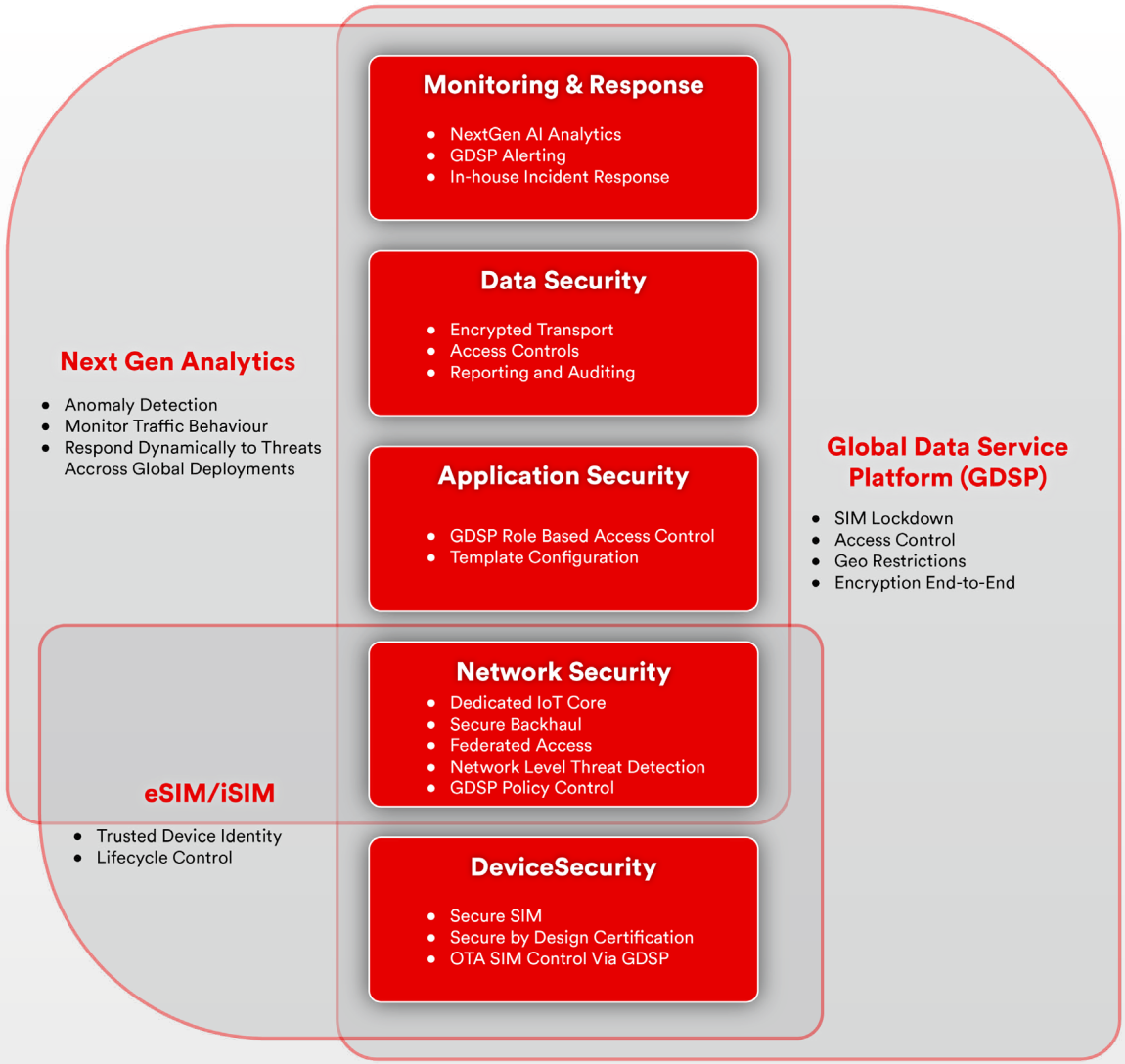
Securing the IoT Technology Stack: Vodafone's Layered Approach

Securing IoT at global scale requires a multi-layered approach that addresses risks across the IoT technology stack. From the device identity and authentication, through to global network transport, data handling, application access, and real-time monitoring and response.

Vodafone IoT has aligned its security strategy to address threats across this stack, integrating advanced security controls into each layer. These controls are not standalone – they converge at the network level, leveraging Vodafone's experience in critical national infrastructure to deliver higher-grade protection than typically found in unmanaged or proprietary IoT connectivity solutions.

Figure 5 visualises this layered security model, with industry best practices across Device, Network, Application, Data, and Monitoring layers. Vodafone IoT brings together its Global Data Service Platform (GDSP), the connectivity management platform developed and maintained by Vodafone IoT, together with NextGen Analytics, dedicated IoT core, and SIM authentication to secure IoT end-to-end. This makes sure that deployments remain resilient, compliant, and trusted.

Figure 5. Vodafone IoT layered security model



1 Device Security: Trusted Identity and Lifecycle Control

IoT security begins with checking that only authorised and verified devices can connect to the network through a combination of SIM technology, remote management, and device certification.

Secure SIM technologies (physical SIM, eSIM, iSIM) conform to global GSMA standards and provide tamper-resistant, cryptographically secure device identities. Vodafone's Global Data Service Platform (GDSP) adds over-the-air SIM state control, allowing Vodafone to activate, suspend, or decommission SIMs remotely to limit exposure from inactive devices.

Vodafone makes sure that only verified devices can access network services.

2 Network Security: Dedicated IoT Core, Encryption and Policy Enforcement

Vodafone IoT's dedicated IoT Core Network separates and isolates IoT data from consumer and enterprise services. Encrypted backhaul helps to protect signalling and data traffic in transit.

Vodafone IoT's converged security model delivers a high standard of network protection and heavily reduces exposure to common threats. Furthermore, peer-to-peer communication is blocked by default, limiting the risk of attacks spreading between IoT devices.

3 Application Security: Controlled Access and Consistent Policies

Vodafone's Global Data Service Platform (GDSP) is the central control hub for IoT connectivity. It acts as a single pane of glass for managing global device fleets – enabling enterprises to provision and manage SIMs, define security and usage policies, restrict network access (via geofencing, firewalls, and APNs), and integrate these controls into business systems through secure APIs. GDSP also plays a vital role in security, with role-based access control, automated alerts, and policy enforcement to help make sure devices remain compliant and protected across their lifecycle.

4 Data Security: Encryption and Oversight

Vodafone IoT integrates security at each step of data protection, from transmission to access control and reporting. Traffic between devices and Vodafone IoT's dedicated core is encrypted, and customer data is stored securely in ISO 27001 and TISAX certified facilities.

5 Monitoring and Response: AI-Powered Threat Detection

Vodafone IoT's layered approach is reinforced by advanced, real-time monitoring and expert incident response. At the heart of this is Vodafone's global Cyber Defence Centre. This team provides 24/7 threat detection, analysing vast streams of data from across Vodafone's networks, platforms, and IoT services to identify and neutralise potential threats.

Securing the connection is critical, but the stack extends into the enterprise and that's why Vodafone IoT provides professional services – helping to manage operational risk, whether this is through application layer security, advising on application and firmware design or operational processes.

Furthermore, Vodafone IoT's AI-powered network anomalies detection tool and the GDSP platform offer additional layers of vigilance. Together, they monitor device and network behaviours in near real time, aiming to raise alerts and automating responses to operational anomalies before they escalate. This multi-layered defence helps to make sure that threats are contained and service restored swiftly – no matter where in the world customers deploy their IoT devices.

Embedding Security by Design and Governance

Vodafone's layered approach is underpinned by a security-first culture. Global certifications, such as ISO 27001 and TISAX, demonstrate rigorous security standards across its infrastructure and platforms. Vodafone actively contributes to global security best practice, currently holding leadership roles in bodies such as ETSI, GSMA, and ENISA.

Vodafone also offers advisory services to enterprise customers.

Key Benefits of Vodafone's Converged Approach

- Unified protection across all technology stack layers, aligned to global security frameworks and rigorous internal standards.
- Robust protection through dedicated infrastructure and telecom operational security.
- Near real-time visibility and control via GDSP and NextGen AI-driven network anomaly detection tool.
- Embedded security culture through certification, governance and industry participation.

Additional References

Cybersecurity Factsheet at this link

Vodafone's Cyber Security Factsheet provides details on the company's approach to managing cyber risk, as well as how it protects customers from online threats:

- Industry-wide collaboration: To encourage standardisation, share intelligence, and engage with key stakeholders on regulation. We collaborate across industry and government so we can be better prepared to manage the threats we collectively face. The backdrop of geopolitical instability, conflict and tensions leads to an increase in cyber threats from state-backed and criminal threat actors.
- Ever evolving defences: Vodafone's cyber security strategy is updated in line with developments in the technology and threat landscape. Given that vulnerabilities are quickly exploited by hackers, Vodafone has processes to respond rapidly, provide effective monitoring and in-depth defence.
- Monitoring AI: As well as countering current threats, Vodafone's approach is to utilise new technologies whilst also tackling the risks they generate, including the use of generative AI.
- Quantum vulnerabilities: Looking further into the future, through Vodafone's joint research with IBM, the company has developed a risk-based approach to post-quantum safe cryptography. This involves identifying potential quantum vulnerabilities, defining supplier requirements, and developing a risk-based model to update Vodafone's cryptography.

These activities are supported by a global team of 900+ cyber experts, including the Cyber Defence Centre, who constantly monitor and proactively defend against threats to the Vodafone network.

Vodafone IoT improves customer experience with AI-powered anomaly detection tool

In December 2024, Vodafone IoT launched its own enhanced anomaly detection tool, powered by AI. This tool uses machine learning algorithms to proactively detect service anomalies in near real time, meaning that customer support teams have instant access to advanced data insights and, as a result, can react faster to any issues.

Cyber Security Centre for SMEs in Germany

In March 2025, Vodafone Germany launched a new Cyber Security Centre in Düsseldorf. This aims to support and protect small and medium-sized enterprises (SMEs), who typically don't have the same resources as large corporations to defend against cyberattacks.