IoT under lock and key

IoT under lock and key: security considerations when deploying IoT

Together we can
vodafone
business

Foreword

Our role is to enable connectivity in society. As a provider of critical national infrastructure and connectivity that is relied upon by millions of customers, we prioritise cyber and information security across everything we do.

Cyber-attacks are part of all our lives today and will be in the future. All organisations, governments and people will be subject to cyber-attacks and some will be successful. The telecommunications industry is faced with a unique set of risks as we provide connectivity services and handle communication data.

The security of our networks, systems and customers is a top priority and a fundamental part of our company purpose. Our customers use Vodafone products and services because of our next-generation connectivity, but also because they trust that their information is secure.

Cyber underpins everything we do across the company.

Our cyber operating model and strategy are designed based on this threat landscape, and we implement controls that prevent, detect and respond to attacks to minimise impact.

Our comprehensive suite of services enables advanced monitoring, increased network reach and secure fixed, mobile and IoT communications.

We follow a security and privacy design process for all components, the platform, the SIMs, connectivity and branded devices - we do this for all our products and services.

We not only understand today's challenges, but we also prepare our customers for tomorrow using advanced security analytics, machine learning and other elements like Next-Generation managed firewalls.

We are proud to supply highly resilient IoT connectivity, wholly managed by Vodafone Business, providing clear visibility and control of IoT devices, SIMs and services which are designed with security built-in from the start.

Is your business Fit for the Future?

In our latest research, we set out to discover which businesses were Fit for the Future (FFTF)[1] – what they do differently to other businesses and how they approach challenges.

We found the best-prepared ones had six key things in common:

Adaptable
They can react quickly to new trends or challenges and are quicker to market than other companies.

Positive attitude to change
They see change as an opportunity and are excited by the future.

Up to date with emerging trends
They work to understand the forces shaping their business and they get help from key thought leaders.

Open to new technology
They understand the power of technology to solve their business challenges.

Plans for technology
They have roadmaps in place for how technology can transform their ways of working.

Detailed strategies
They have wider business strategies for the future that are documented, specific, funded and measured.

FFTF businesses also see more opportunities in IoT technology

Especially when it comes to using IoT technologies for monitoring, optimising, automating processes and quality control. While 31% of businesses say that using data collected by IoT systems is a challenge, 44% of FFTF businesses say IoT has exceeded their expectations – and that their IoT budgets have shot up as a result.[1]

So, what does this mean for you?

If your business isn't already using IoT, it probably will be soon

But what's the best way to embrace IoT while protecting your data and your customers?

We spoke to over 1,500 decision-makers, across a range of business sizes, about their technology and found while 37.9% worry about IoT security (and this was most important for businesses with 1000+ employees), 48.5% of existing IoT users are more concerned with having the right expertise. This shows that although security isn't a major concern, it's still a key part of the decision process.

So whether you are considering IoT or looking to enhance your security systems, here are the **six key questions** business decision makers thought it most important to ask:

01 **Will our IoT data be protected?**

02 **Could hackers take control of our IoT devices?**

03 **Could SIM fraud cost our business money?**

04 **How do we get the skills we need in our teams?**

05 **Will our business kept secure wherever we operate in the world ?**

06 **How can we control access to our business?**

Source:
[1] Vodafone Business Fit for the Future
Primary research conducted by Vodafone Business, 2023

01. Will our IoT data be protected?

IoT's business value lies in the data it gathers — data that's often mission critical and collected at scale. We protect it from theft or tampering as it moves over the network.
Here's how.

Your data is always under our protection

IoT data comes from devices like smart meters, solar panels, vending machines and payment terminals, and often has to travel a long way back to the data centre. If a breach happens at any point in that journey, sensitive data is at risk.

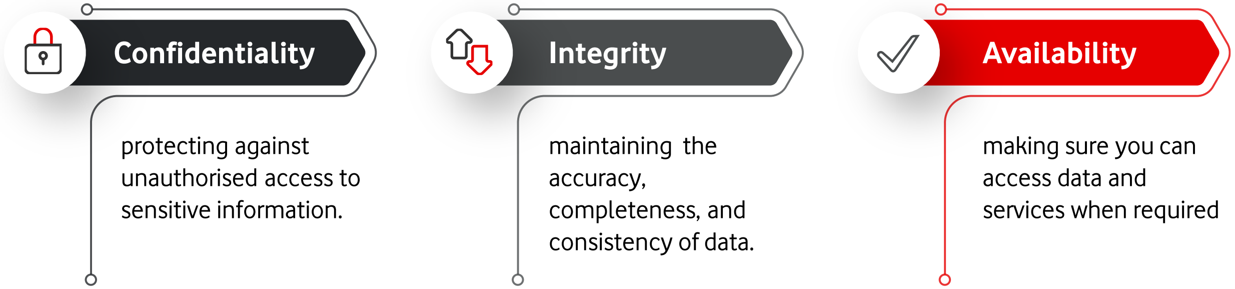
We include resilient measures for device authentication and secure authentication - even before the device is allowed to transmit.

We offer hosting and private cloud environments for your applications, too. Or, if you'd prefer to host your applications somewhere else, there's a range of secure backhaul connections between our data centres and yours to choose from.

All of this adds up to seamless security, without any of the risks that come from integrating solutions from different providers. It also makes us more accountable. We look at the risks your data could face from all angles. And if we need to make a change to protect your data from a threat, we're able to do it – and fast.

We wrap your data in multiple layers of protection

Confidentiality, Integrity and Availability are the three points of the CIA Triad information security model, which many businesses like ours use to guide their security standards.



Confidentiality

protecting against unauthorised access to sensitive information.

Integrity

maintaining the accuracy, completeness, and consistency of data.

Availability

making sure you can access data and services when required

In our IoT infrastructure, we use these measures and more.

For example, every time an IoT device tries to open a data session on the network, we authenticate it using cryptographic keys in the SIM. And whenever a user tries to connect to our Managed IoT Connectivity Platform, we only let them in through proven security techniques, such as two-factor authentication and strong passwords over HTTPS.

We also separate our IoT subscribers from public internet traffic and encrypt all the data that passes over our mobile networks. To give you an extra layer of protection, we provide application-layer end-to-end data encryption from the device to your applications. This authenticates the device's identity – and safeguards sensitive data against unauthorised access.

Will our IoT data be protected? continued

A global security team dedicated to reducing cyber risk for customers

Our Cyber Security Team reports directly to our CTO. It's their job to make sure we follow our security processes to the letter.

We align our policies with international standards from organizations such as ISO[3] and NIST[4],

We don't just set and forget our security standards. We review and update them regularly to stay up to date with what our customers need and the threat environment. As part of our compliance certifications, we get our network elements, data centres, offices and shared services centres regularly independently audited. We've also recently renewed our ISO 27001 certification. You can find out more about our cyber security strategy here.

Our cyber security strategy

Our vision is a secure, connected future for our customers and society. Our cyber security strategy[5] sets out how we plan to get there. It is aligned to, and forms part of, our technology strategy:

Control evolution: Maintain and improve our security controls beyond the existing cyber security baseline with an adaptive and risk-based framework.

Real-time data, real-time response: The next generation of our detection and response capability, more automated and based on advanced analytics.

Secure by design: All products and services have security built-in whether we build them ourselves or buy them from vendors.

Spirit of Vodafone & cyber culture: Engaging our people, nurturing our engineering community and Group-wide cyber security training and simulations.

Dynamic Trust: Strong zero-trust security based on dynamic risk-based access, which is frictionless for users, for example, multi-factor authentication and moving away from passwords.

Security for society: Collaborate widely to encourage standardization, share intelligence, and engage on regulation.

Each year we define and communicate priorities for a three-year period, so all areas of our business are clear on the investment priorities for security.

Also core to our strategy are the wider Vodafone sustainability goals. We're committed reaching net zero emissions by 2040, while helping our customers reduce their own carbon emissions by 350 million tonnes by 2030. We're driving action to reduce device waste and achieve our target to reuse, resell or recycle 100% of our network waste by 2025.

Source:
[3] https://www.iso.org/isoiec-27001-information-security.html
[4] https://www.nist.gov/
[5] https://reports.investors.vodafone.com/link/516156/1/

02. Could hackers take control of our IoT devices?

Sometimes all it takes for a hacker to cause damage is a single slip, whether that's a misconfigured router or weak user credentials. Here's how we can help you protect devices that connect to our IoT environment and minimise the risks to your business.

We build security into our Vodafone branded devices

We only work with selected manufacturing partners to design and build our Vodafone-branded IoT devices. We're always looking for ways to make our devices more secure: from tamper-resistant casings to hardened firmware configurations.

We also offer a secure supply chain service, including manufacturing, configuration and dispatch. And because our devices arrive ready to use, it reduces the risks that come with trusting a third party with the setup.

Put your devices to the test

If you're building your own IoT devices, or working with a manufacturer, we can help you choose your hardware. Through our professional services packages we can also support making your device and its connected environment more resilient to security threats.

You can also try out and certify your devices on the sandboxed network at our test and innovation centre (VIP labs) – giving you the chance to identify and solve any connectivity glitches before you use them in the field.

Put restrictions in place

Even the most hardened device shouldn't be given unrestricted access to the rest of your IoT environment, so we tightly control how each device connects.

Devices fitted with a Vodafone Business IoT global SIM use a private network to connect to our platform and are assigned a private, unpublished IP address. We can also protect IoT devices through multiple layers of security such as firewalls and rule-based mechanisms, along with private connectivity, such as private access point names (APNs), to your data centres.

03. Could SIM fraud cost our business money?

Imagine: you've got tens of thousands of IoT traditional SIMs out in the field. What if someone harvests them, tries to put them in other devices, and starts racking up data charges? We help you reduce the risk of that happening through security features on our SIMs including our SIM limits and protecting access protocols, IMEI locking, and more.

Deploy

Use integrated SIMs

Anyone would struggle to find one of our iSIMs (integrated SIMs), let alone remove it.

iSIMs are a new type of SIM providing the same functionality as standard plastic or robust SIM, however, from the physical point of view they are very different. iSIMs are tiny, embedded inside trusted areas of other chips, which are in turn soldered directly to your device's circuit board making them incredibly difficult to harvest.

Restrict the services SIMs can use

Each SIM is assigned a tightly managed set of services it can access. Packet data is standard, whereas SMS and voice are optionally available.

The network locks each SIM to the agreed IoT APN we configure for you in our IoT platform. When any IoT device tries to connect to the network, its SIM is checked and its data connection is authenticated using 3GPP standards. This is done through the subscriber key, which is built into each SIM when it's manufactured — a unique advantage of mobile connection.

Only known SIMs can connect. And each known SIM can only connect to the services you've defined. This is also true if the device isn't configured with the APN name stored in its firmware. So even if someone tampers with the IoT device, you keep total control over service access.

Manage

Take control of all your SIMs together

It doesn't matter how many IoT SIMs you have — you control all of them in one place with our platform, which scales to millions. It includes test, suspended or deactivated SIMs as well as live connections. And it includes SIMs on any network around the world.

Plus, if it's a Vodafone Business Global IoT SIM, you'll be able to manage it in near-real time. So, if one SIM starts to act differently, you can shut it down immediately.

04. How do we get the skills we need in our teams?

As IoT gets bigger and more complex, your internal IT teams might need extra support or specialist advice. We can help.

Choose simple solutions that are easy to manage

We're the largest global IoT provider, and are able to connect devices in 190 countries, meaning you don't have to juggle different suppliers or stocks for different regions – or deal with the complex supply chains that come with it. And our devices and connected products come ready to use straight from the box, saving you time on setup and cutting the risk of human error.

Our Managed IoT Connectivity Platform gives you a single portal interface and a range of APIs, so you can manage all your connections in one place. And because the Platform is a hosted service, you don't need to worry about securing it like you would if you were hosting it yourself. It's run from our ISO 27001-certified data centres, and we take care of all your physical and network security, backups, and business continuity. Plus our ITIL, Prince2 and CMMI qualified experts have got your back at every stage.

Get support from signup to setup and beyond

You can trust our people like you trust your own. We use an independent service provider to run background checks on all our employees. Many of our teams are security cleared at the highest level of government.

We always restrict access to systems and data to a need-to-know basis and monitor our employees' access to all IoT systems. And if we ever need to bring in a third party, we audit them to make sure their standards are just as high as our own.

Help yourself to our knowledge store

We invest a lot in our IoT and security teams. Because only by building a pool of first-class knowledge can we stay ahead of increasingly capable threats.

Today, our IoT business has more than 1,400 experts, with many with years of experience. We also employ around 800 people worldwide to protect our customers' privacy and personal data.

Our security experts play a leading role in the industry, sharing insights and developing new standards that help everyone. For example, we collaborate with organisations like ETSI, GSMA, ENISA and 3GPP — in particular, leading the GSMA Fraud and Security Group. We're also a founding member of the Global Forum on Cyber Expertise, and we sit on the Executive Steering Board of the IoT Security Foundation.

05. How is our business kept secure wherever we operate in the world?

Our Cyber Code

In 2019, we launched the Vodafone Cyber Code, which has been designed to simplify and explain the basic security controls to all employees. Embedded in our Code of Conduct, the Cyber Code is the cornerstone of how we expect all employees to behave when It comes to best practice in cyber security.

✓ **ALWAYS**

- Use multi-factor authentication for remote systems that hold sensitive information.
- Apply the latest security patches, close critical and high vulnerabilities and configure systems securely.
- Remove access when staff change roles or leave Vodafone. Secure privileged access and only use it for privileged tasks.
- Classify, label and protect information you work with.

✕ **NEVER**

- Allow unsupported end of life systems in Vodafone infrastructure or release unsecured products or services.
- Click on links or download without knowing who it is from. Report suspicious behaviour.
- Share or reuse your passwords. Longer is stronger.

Security is challenging enough without the added complexity of working across different regions and legal jurisdictions. Here's how we deliver constant protection for every IoT project.

Set consistent policies and processes

Striking the right balance between global consistency and localisation isn't easy. We understand - we have business operations, relationships and partnerships in 65 countries, and customers in dozens more.

So we use global, group-wide processes and policies to keep us consistent. We follow the strictest 3GPP standards for infrastructure no matter where it's deployed, and whether it's used for consumer, enterprise or IoT purposes. We support (and whenever we can, surpass) international standards, like ISO 27001 for data security, ISO 22301 for business continuity and TISAX for the automotive market. We're also active in the standards bodies that define best practice.

Our legal teams across our Group keep us compliant with local laws, and as a European-based provider we're subject to some of the world's most stringent security, privacy and compliance laws. This sets us up for meeting other regulations around the world.

For example, we're a founding member of the IoT Security Foundation, a not-for-profit that comes up with principled and systematic ways to deal with government demands that could affect privacy and freedom of expression.

Trust in our network and critical-industry expertise

As one of the world's largest telecommunications operators, our IoT platform scales to the number of devices owned by the customer while giving centralised control.

We've engineered our infrastructure to be secure and resilient. For example, our core network has secure network gateways embedded within it. This gives next-generation firewall and intrusion detection to protect against advanced threats on a global scale. The data centres that host our Managed IoT Connectivity Platform are certified to ISO 27001 standards. Our IoT platform, portal, API and associated systems are implemented across global sites with redundant hardware setup and automatic failover. We've based each hosting site on a tiered architecture model of discrete security zones, with strong firewall separation between each zone, state-of-the art intrusion detection systems, and individual host-based controls. The result is an infrastructure and applications that are both local and geo-resilient able to withstand incidents and ready for disaster-recovery events.

For more than 30 years, we've been the service provider for businesses across critical industries like healthcare, government, emergency services, automotive and utilities have turned to. They trust us to deliver, not just their fixed and mobile communications, but to also host their applications in our cloud and run their IoT business.

Nothing can be left to chance. As a provider of critical national infrastructure ourselves — the telecommunications network — we know this better than anyone.

06. How can our business keep control?

Any security expert will tell you: whatever controls and layers of protection you put in place, there's no such thing as perfect security. Proactive monitoring is a vital part of the overall IoT environment – spotting problems and acting before damage is done.

Be picky about who has access

Nobody likes to think about the disruption a single employee can cause – deliberately or by mistake. Our user access controls let you limit who can access the management portal by role. Activity is logged for forensic investigation, and users are verified with two-factor authentication.

Stick to the control and risk framework

We can prevent most risks from occurring, and we detect most threats before they cause harm. A small minority will need response and recovery actions.

We use a common global cyber security methodology, the Cyber Health and Adaptive Risk Method (CHARM). This has been designed to adapt to the changing threat environment, prioritise the most important controls and enable risk-based decisions through KRIs and automated reporting. The security controls that make up the control framework are based on international standards and include security controls to prevent, detect, and respond to events and attacks. We continuously monitor how our controls are performing, and the control framework itself is regularly reviewed with new controls and targets added to keep pace with the evolving threat landscape. You can read more about our risk and control approach in the 2024 Cyber Factsheet: here.

We're as selective about who we work with as you are

We only work with suppliers who take cyber security as seriously as we do.

When we onboard a supplier, we write security requirements into contracts and work out a supplier's inherent risk based on the service they're providing and information they are handling. We then assess their controls to understand the residual risk, which tells us how often to review them. We follow up on open actions and make sure we track and manage security incidents to resolution and reflect on lessons learned.

The Cyber Security Operations Centre (CSOC): your eyes on the ground

Our experts monitor traffic and watch for security incidents across our network. If they detect a cyber threat, they respond in real time to minimise its impact. They deal with tens of millions of security events every month, to keep our network running smoothly and protect the privacy of over 330 million individuals. But no matter how tough your security, some attacks might be successful, affecting services and compromising data. If the worst does happen, our business continuity management team will alert you and work with you to develop your response. We align our business continuity management with International Standards, such as ISO 22301, and with local legislation.

Think self-sufficient when it comes to monitoring

Your IT and security teams need to be able to see how your IoT devices are functioning and respond to issues without having to call us.

Our Managed IoT Connectivity Platform gives you an up-to-date view of the operational status of each connected device. This includes its data usage, billing status, and, in some cases, a precise location reading.

You can monitor through our network and spot where services are being used unexpectedly or excessively. This will trigger an alert on the portal and an email. You can use the portal to lock down any compromised device with the click of a button or configure rules to automatically disable any device that's behaving unusually.

Look to the future, together

We have big plans for the next few years.

As well as maintaining our cyber security baseline controls – especially around software security, multi-factor authentication and protecting against ransomware – we're modernising our security event monitoring and data analytics platforms.

We're enhancing our coverage for managing privileged access to network and IT systems and introducing risk-based access rights for our employees. We'll also continue to enhance our cyber security awareness programme and put more of our people through it.

As the IoT landscape evolves, our focus remains on staying ahead and anticipating our customers' needs. This is why we continually invest in innovation and enhancements, such as our IoT Connectivity Portal 2.0 platform, which offers a seamless user experience and improved functionality, as well as our IoT Analytics service that delivers real-time insights and actionable recommendations.

We believe these initiatives enable us to provide greater value and foster more growth opportunities in the IoT sector.

What's next?

So where do you start? Every business is different, and your risk landscape will be unique to you. The security measures you put in place should align to those risks – and your budget.

So, if you're developing your IoT strategy to make security an integral part of your operations, talk to us.

We'll deliver the protection that's right for you.

✉ Get in touch

Our leading experts are on hand to provide advise based on your business requirements.

Email us at iot@vodafone.com and our IoT Specialists will guide you on your next steps.

www.vodafone.com/business/products/iot-connectivity

Together we can

vodafone
business