Securing the Internet of Things

An overview of how Vodafone is working to keep connected devices and people's data safe in a changing world.

vodafone.com/iot

The future is exciting.

Ready?

vodafone

Demystifying IoT security

Every day businesses come to us wanting to know what adopting IoT will mean for their security, privacy and operational continuity.

This short paper summarises our responses to the six most common questions we're asked. It gives business decision-makers an overview of some of the approaches we take to protect our customers' devices and data.

Security is deeply embedded in all areas of our business, and we're constantly evolving our technology, processes and detection capabilities to stay ahead of the state of the art. If you or your team want to understand more about our security controls, services and expertise, get in touch with your Vodafone account manager.

Contents

Data security is only part of the picture

When you're gathering, storing and processing data from millions of IoT endpoints, it's not just the security of that data against theft and sabotage that you have to plan for. You must also pay attention to business continuity, planning for any eventuality (accidental or malicious) that could disrupt service. And, crucially, you have to consider data privacy: making sure that your use of information, particularly about people, is both compliant with local laws and in line with the expectations of your customers and users.

Protecting the privacy of our customers is one of our key missions. We carry the personal data of more than 515 million individuals, every day. People around the world trust us to respect their wishes, and we work hard to live up to that trust. When you choose our IoT services to carry data about your customers, you know that we take their privacy just as seriously.

Background: What businesses really think about IoT security

In our annual IoT Barometer[1], we ask more than a thousand business decision-makers about their views on security. There's evidence of concern — but optimism, too.

Cause for alarm?

In our 2016 report, 18% of businesses said that concern about security breaches is a potential barrier to wider adoption of IoT in their organisation. 30% said they were changing or restricting the scope of IoT projects to limit security risks. And more than half of businesses we talked to said they're more concerned about IoT security risks than they were in the past.

The concern they're feeling is understandable: we've all read stories about IoT door locks that transmit passwords in plain text[2], baby monitors that can be hijacked over the internet[3], and security cameras and digital video recorders that can be joined into a botnet and used to launch crippling denial of service attacks[4]. CIOs and CEOs are right to ask: "What if our IoT devices are as vulnerable?" A hack on a connected car could result in harm to a customer.

In all areas of IT, it's always wise to take security concerns seriously — there are many well-motivated and talented hackers out there, and sometimes all it takes for them to cause damage is a single weak spot, whether that's a misconfigured router or weak user credentials. Businesses can't afford to let their guard down for a second.

Reason for confidence

But when it comes to IoT, the reality is less sensational than the stories suggest, and not all IoT deployments are equally at risk.

The baby monitors and wireless security cameras that hit the headlines after the Dyn breach generally use unsecured, unmanaged public internet connections and have been designed and configured without sufficient consideration for data security. They're in a completely different league from a true enterprise-class IoT deployment managed by a reputable provider — such as Vodafone. Not all IoT solutions are created equal.

Companies that take security seriously are addressing the risks and moving forward with confidence, and we found evidence of that attitude in the Barometer. 75% of businesses we talked to consider security risks to be a "fact of life". The vast majority were already factoring security into their projects — for example, by making data security a major part of their RFP requirements for new projects.

18% of businesses said that concern about security breaches is a potential barrier to wider adoption of IoT in their organisation.

75% of businesses we talked to consider security risks to be a "fact of life".

30% of businesses said they were changing or restricting the scope of IoT projects to limit security risks.

To learn more about how enterprises are using IoT today, **click** to download the Vodafone IoT Barometer 2016.

“Will my IoT data be vulnerable?”

IoT’s business value lies in the data it gathers — data that’s often mission-critical and on a tremendous scale. We help protect that data from theft or tampering as it moves over the network.

1. Owning the infrastructure for seamless security

IoT data originates at the very edge of the infrastructure, far beyond the protection of the corporate perimeter, in remote devices like cars or security cameras. It’s a long journey to the data centre. If a breach happens at any stage in that journey, sensitive data is at risk.

That’s why we take responsibility for securing the data as it moves from the SIM, or embedded SIM, in the device through the wireless and core networks around the world, to the central management platform and the data centres where it’s hosted.

We can even provide hosting and private cloud environments for your applications so your data never has to leave our protection. Should you wish to host your applications elsewhere, we offer a range of secure backhaul connections between our data centres and yours.

All of this means you benefit from seamless security, without the risks associated with integrating solutions from multiple providers. It also means you benefit from greater accountability and agility. We have a holistic view of the risks facing your data, and are empowered to make any changes that we need to, at speed, to help minimise the risks to your systems.

76% of businesses say that IoT security should be treated as an end-to-end solution, and **91%** say it is important for them to work with an end-to-end solution provider for IoT.

Vodafone IoT Barometer 2016

2. Supporting multiple layers of data protection

In any IT system, data protection is achieved by encrypting data, by isolating systems from each other, and by restricting access through authentication and authorisation controls. This isn’t an exhaustive list of controls. We use these and more in our IoT infrastructure.

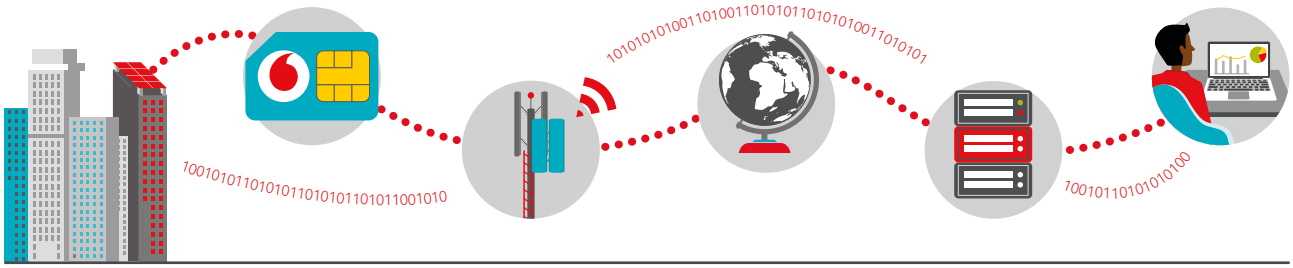
For instance, every time an IoT device attempts to open a data session on the network, we authenticate it using cryptographic keys in the SIM. At the other end of the data journey, whenever a user attempts to connect to our web portal, we authenticate them using two-factor authentication and strong passwords, over HTTPS.

We also separate our IoT subscribers from public internet traffic, and encrypt data that passes over our mobile networks into the network core by default. As an additional layer of protection, we support and strongly recommend application-layer end-to-end data encryption from the device to your applications.

3. Planning and testing for end-to-end security

Security is too important to be left to chance. That’s why we operate a specialist security function responsible to the CEO of Vodafone. This team maintains our security policy framework, covering all aspects of security, privacy and compliance. Our policies and our security control framework are aligned with international standards from organisations such as ISO[5] and NIST[6], so they’re robust and comprehensive.

We don’t just “set and forget” when it comes to security. We review and update our policies regularly to stay current with the needs of our customers and the threat environment. As part of our compliance certifications, our network elements, data centres, offices and shared services centres are regularly independently audited.



“Could hackers take control of my IoT devices?”

Whether it’s a baby monitor or a connected car, it’s the edge device that’s most visible and exposed as a target for hackers. Here’s how we protect devices that connect to our IoT environment to minimise the risks to your business.

1. Building security into our Vodafone-branded devices

We offer a range of Vodafone-branded IoT terminals that you can use to add IoT connectivity to your assets, such as the MachineLink 4G. Each of these terminals has been designed by us and built to our specifications by carefully audited manufacturing partners. We’re constantly working to further strengthen security across the designs: from tamper-resistant casings to hardened firmware configurations.

For these Vodafone devices, we also provide a secure supply chain service, including manufacturing, configuration and dispatch, so that devices can be delivered ready to deploy. This minimises the risks associated with interception or configuration.

2. Offering professional services to help you select secure designs

If you’re building your own IoT devices, or working with a hardware manufacturer to do so, we offer a range of professional services to help you select hardware and harden your devices to limit the threat from known security vulnerabilities.

We also make available our test and innovation centre for pre-deployment testing. We offer a robust and repeatable test environment that enables you to identify any potential issues ahead of deployment by trying out your devices on a sandboxed network.

For more details about our professional services, take a look at our brochure.

3. Restricting the way devices access the network and communicate over it

Even the most hardened device shouldn’t be allowed unrestricted access to the rest of the IoT environment. We operate a minimal trust model and tightly control how each device connects.

Each IoT device fitted with a Vodafone IoT global SIM uses a private network to connect to our platform. Each is assigned a private, unpublished IP address; it’s not discoverable from the public internet. The service can shield IoT devices from the public internet and from access through your corporate network using a variety of firewall and rule-based mechanisms, coupled with private connectivity to your data centres.

Should a hacker access and breach an individual device, the implementation of private access point names (APNs) within the IoT core helps prevent that device being used as a gateway into the rest of your network.

“Could fraudulent use of my IoT SIMs cost me money?”

Imagine: you’ve got tens of thousands of IoT SIMs out in the field. What if someone harvests them, puts them in other devices, and starts incurring long-distance call charges or data bills? We can help you reduce the risk of that happening.

1. Using tamper-resistant SIMs

Vodafone IoT SIMs are fundamentally different to standard SIMs. In addition to offering “standard” plastic SIM formats for IoT deployments — following ISO/ETSI standards, including in rugged formats — we also provide embedded SIMs, known as eSIMs. These chips are tiny and are soldered directly to your device’s circuit board. It’s difficult for hackers to even identify the eSIM, let alone physically remove the SIM and try to put it in a phone.

2. Restricting which services SIMs can use

We help prevent fraud by limiting what each SIM is allowed to do. By default each SIM is assigned a tightly managed predefined set of data, SMS and voice services that it can access, and a selected list of mobile networks that it’s allowed to use.

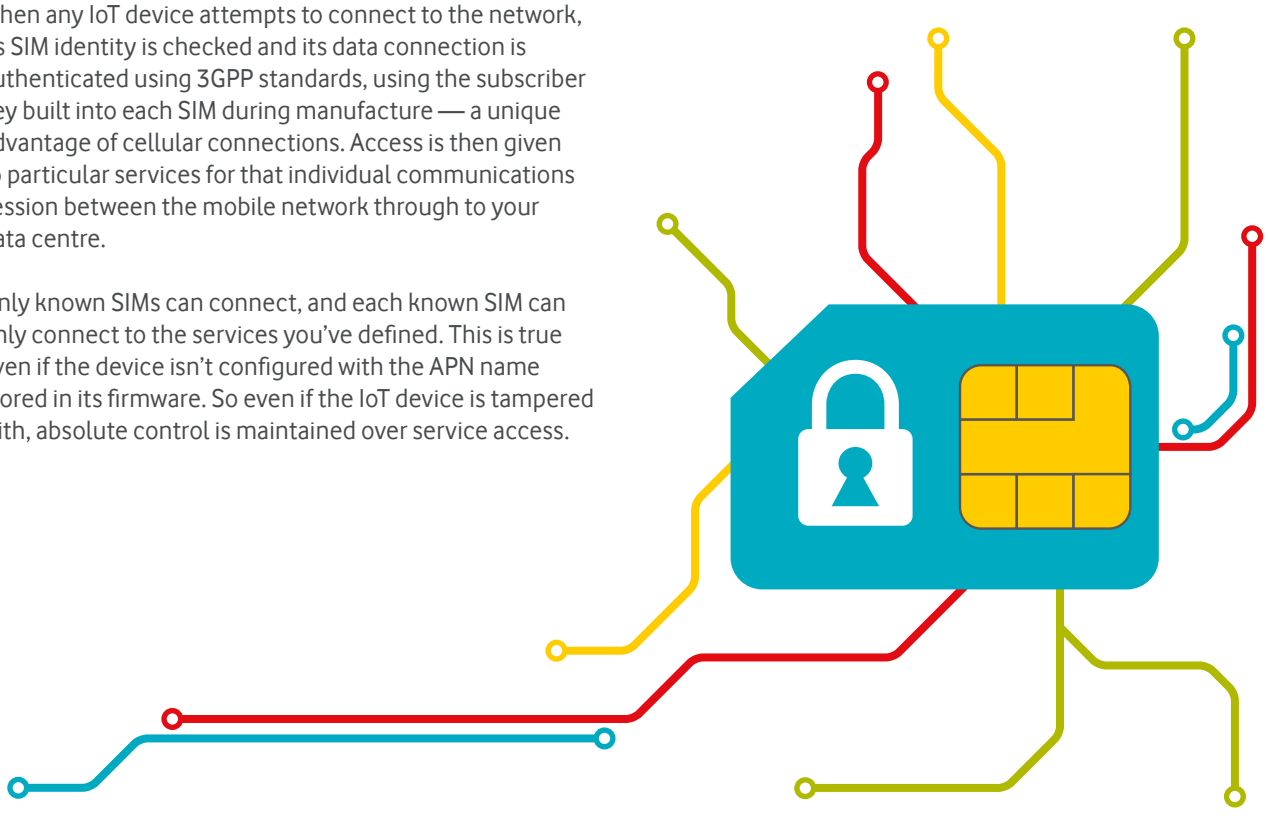
Each SIM is locked by the network to the specific private IoT APN that we configure for each customer in our IoT core. When any IoT device attempts to connect to the network, its SIM identity is checked and its data connection is authenticated using 3GPP standards, using the subscriber key built into each SIM during manufacture — a unique advantage of cellular connections. Access is then given to particular services for that individual communications session between the mobile network through to your data centre.

Only known SIMs can connect, and each known SIM can only connect to the services you’ve defined. This is true even if the device isn’t configured with the APN name stored in its firmware. So even if the IoT device is tampered with, absolute control is maintained over service access.

3. Giving you centralised control

With our IoT platform, you have complete control of all your IoT SIMs in one place. This applies no matter how many SIMs you have — the platform scales to millions of connections. It includes SIMs that are suspended or deactivated, as well as live connections. It includes 2G, 3G, 4G, NB-IoT and satellite SIMs. And it includes SIMs that are on any Vodafone network or other operator’s network around the world. If it’s a Vodafone Global IoT SIM, it will be manageable in near-real time from our platform. That means if a SIM goes rogue, you can see it and shut it down immediately.

Find out more about our Managed IoT Connectivity Platform at **vodafone.com**.



“How do I get the skills I need in my team?”

As IoT deployments grow larger and more complex, your internal IT teams may need additional resources or specialist advice to secure your deployments. We can help.

1. Reducing the burden with simplified management

One of our key design principles is to make our solutions as easy to manage as possible. For instance, our SIMs work globally, meaning you don’t have to manage different suppliers or stocks for different regions, or the supply chain complexity that comes with it.

If you choose our integrated terminals or connected products, we ship the hardware with connectivity preinstalled and preconfigured, minimising setup time and avoiding human error. Our Managed IoT Connectivity Platform gives you a single portal interface and a range of APIs to manage all your IoT connections from one place.

And because the Platform is a hosted service, run from our ISO 27001-certified data centres, you don’t have to worry about securing it, as you would if you were hosting it yourself. We take care of physical and network security, backups and business continuity. And at every stage of development and operations, our ITIL, Prince2 and CMMI qualified experts help deliver a consistent outcome.

2. Supporting you with end-to-end professional services based on best practices

You may need specialist skills and additional resources at several stages during a project: solution design and testing; implementations and integration; major upgrades or migrations; and so on. In these cases, we can offer a range of professional services to supplement your internal teams. As well as providing more general advice and support, our services can help you achieve your goals for protecting your business. We can advise on everything from hardware configuration to the compliance requirements of different jurisdictions.

We take every step to ensure that, when you let us into your business, you can trust our people as implicitly as you trust your own. Our HR teams use an independent external service provider to perform security screenings and background checks on all our employees. Many of our teams are security cleared at the highest level of government.

We restrict access to systems and data within our business at all times on a “need to know” basis, and monitor access by our employees to all IoT systems. Where we engage third parties, we audit them thoroughly to make sure they live up to our high standards.

3. Building a store of knowledge to share with you

We invest heavily in our IoT and security teams. Only by recruiting and developing a pool of first-class knowledge can we stay ahead of increasingly capable threats.

Today our IoT business has more than 1,400 experts, many with years of experience navigating the complexities of IoT implementations. We also employ around 800 people worldwide whose roles are wholly or partly focused on protecting our customers’ privacy and personal data.

Our security experts play a leading role in the industry, to share insights and develop new standards that benefit everyone. For instance, we take an active part in bodies such as ETSI, GSMA, ENISA and 3GPP — in particular, leading the GSMA Fraud and Security Group. Vodafone is also a founding member of the Global Forum on Cyber Expertise, and we sit on the Executive Steering Board of the IoT Security Foundation.

In our 2016 Barometer research, we asked organisations to rank their top three reasons why they’re concerned about IoT security. The top concern was that IoT security is an “unknown quantity”. Second is that the complexity of IoT deployments is making it harder to manage risks.

“How can I secure global deployments?”

Security is challenging enough without the complexities of managing deployments across different regions and legal jurisdictions. We can help deliver consistent protection for even the most business-critical IoT projects.

1. Setting consistent policies and processes that meet local needs

Vodafone has direct business operations in 26 countries, and relationships, partnerships and customers in dozens more. We understand the intricate balance between global consistency and local needs, particularly when it comes to large-scale multinational deployments and how they’re affected by different standards and laws.

We use our global, group-wide processes and policies to enforce consistency in how we do business. Within the network, 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 aim to exceed international standards, such as ISO 27001 for data security and ISO 22301 for business continuity. We’re also active in the standards bodies looking to lead the way in defining best practice.

As a European-based provider, we are subject to some of the most stringent regulations and customer scrutiny in areas of security, privacy and compliance, which sets us up well for meeting requirements right around the world. And we have legal teams across our group to keep us compliant with appropriate local laws. But we always act to represent the interests of our customers and their users.

For example, Vodafone is a founding member of the Telecommunications Industry Dialogue[7] and a signatory to its Guiding Principles on Freedom of Expression and Privacy[8]. These define a common approach to dealing with demands from governments that may affect privacy and freedom of expression in a principled, coherent and systematic way.

2. Operating scalable, resilient and secure global networks and data centres

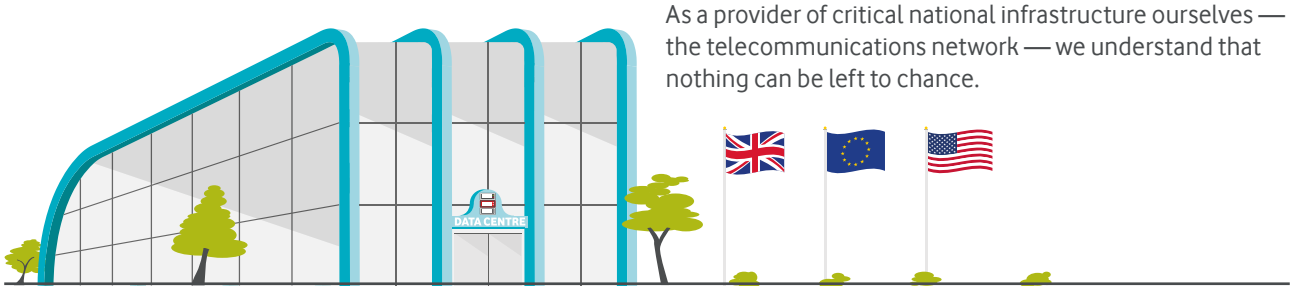
As one of the world’s largest telecommunications operators, we have a truly global presence and the scale to handle even the largest business requirements. And IoT is no afterthought in that presence. We’ve designed our core network for the specific traffic needs of IoT solutions. Our IoT platform scales to millions of devices per customer while giving centralised control.

We’ve set out to engineer our infrastructure for security and resiliency. For example, our core network has advanced secure network gateways embedded within it, providing 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 geographically separated sites with redundant hardware setup and automatic failover. Each hosting site is based 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.

3. Leveraging extensive expertise in critical infrastructure

Vodafone is the first choice for some of the largest and most discerning businesses in critical industries like healthcare, government, emergency services, automotive and utilities. For more than 25 years they’ve trusted us to deliver not just fixed and mobile communications, but increasingly to host their applications in our cloud, and run their IoT deployments. We have deep experience in service delivery on a global scale, meeting high standards for service availability, performance and scalability.

As a provider of critical national infrastructure ourselves — the telecommunications network — we understand that nothing can be left to chance.



“How do I 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. Monitoring is a vital part of the overall IoT environment, improving your ability to spot any problems and take action before damage is done.

1. Continuously monitoring all traffic and network performance on a global basis

Our experts continuously monitor traffic and watch for security incidents across our network from our Global Security Operations Centre (GSOC). The GSOC is designed to detect attacks as they happen and minimise their impact by responding in real time to cyber threats, such as denial of service attacks. We identify and deal with tens of millions of IT security events every month, to keep our network running smoothly and protect the information of over 515 million customers.

We recognise that some attacks may be successful and result in services being affected or data being compromised. We have a robust business continuity management programme across Vodafone to monitor for breaches, outages and other events that affect service, proactively notify customers, and ensure an effective and timely response to any crisis involving critical business operations. We align our business continuity management with International Standards, such as ISO 22301, and with local legislation.

2. Giving customers self-service monitoring, alerting and control

It’s important that IT operations and security teams within your business have continuous visibility of how your IoT devices are functioning, and the ability to respond immediately to an issue, without having to pick up the phone to us. To this end, our Managed IoT Connectivity Platform gives you an up-to-date view of the operational status of each connected device, its data usage, billing status, and in some cases a precise location reading.

The Vodafone network core can be monitored using business rules to identify where services are being used unexpectedly or excessively, triggering alerts on the portal and via email. You can use the portal to lock down any compromised device with the click of a button, or configure sophisticated rules to automatically disable any device exhibiting unusual behaviour.

3. Giving customers strong control over which users and applications can access our APIs and portal

Nobody likes to think about the disruption that a single employee can cause to critical systems, whether deliberately or through error. We provide comprehensive user access controls, enabling you to limit which individuals can access the management portal. Access rights can be limited by role. All access and activity is logged for forensic investigation, and users are verified with two-factor authentication — one authentication method is always certificate-based.

Take advantage of IoT with confidence

76% of businesses say that IoT will be critical to the future success of any organisation in their sector[1]. If your business isn't already using IoT, it probably will be soon. But it's a fact of life that every new technology comes with new risks and threats.

Nobody can guarantee absolute security against these threats. But you can take precautions to protect your operations, your data and your customers against deliberate attack, accident and disaster.

Through our unique owned end-to-end platform, leveraging of industry standards, global scale and deep expertise we believe that Vodafone offers a stronger security proposition than any other IoT service provider. If you're concerned about how adopting IoT might expose your business to risk, we can help.

So where do you start? Every business is different, and when you're adopting IoT your landscape of risks will be unique to you. The security measures you put in place should align to those risks and to your attitudes and budgets. So when you're first developing your strategies for IoT, make security an integral part of those early plans — and talk to us about what we can do to deliver the protection that's right for you.

About Vodafone

IoT projects can be challenging. At Vodafone, we aim to make it easy. Here are three simple reasons why you should partner with us.

1 Unrivalled IoT experience

Vodafone has more than 1,400 dedicated IoT experts that you can rely on. We've been delivering IoT solutions to our customers for more than 25 years and have over 50 million IoT connections. Vodafone has consistently been recognised for our IoT expertise, by our clients and peers. We've been highly rated by leading industry analysts such as Analysys Mason and Machina Research and have been positioned as a Leader in the Gartner Magic Quadrant for Managed Machine-to-Machine Services for three consecutive years.

2 Global networks you can rely on

Vodafone Group has mobile operations in 26 countries, partners with mobile networks in 48 more, and fixed broadband operations in 17 markets. As of 31 March 2017, Vodafone Group had 515.7 million mobile customers and 17.9 million fixed broadband customers, including India and all of the customers in Vodafone's joint ventures and associates. Our scale doesn't just give you the confidence that we operate wherever you do business — it means we can offer the exceptional levels of service you need.

3 The solutions to simplify IoT projects

We have delivered IoT applications for organisations of all sizes and across all industries, so we know how to make your IoT solution deliver maximum value for you. We partner with the world's leading connected device makers to offer a wide range of out-of-the-box IoT solutions that take the complexity out of IoT deployment. But even when you need a customised solution, our team of experts will ensure your business takes advantage of best practices and methodologies for IoT implementation to ensure you achieve maximum ROI.

Next steps

Contact us at **iot@vodafone.com**, call us on 07444 325793 or speak to your account manager to schedule a technology briefing, or to visit one of our facilities to see our security measures first-hand.

References

1. http://www.vodafone.com/business/iot/the-iot-barometer-2016
2. https://techcrunch.com/2016/08/08/smart-locks-yield-to-simple-hacker-tricks/
3. https://information.rapid7.com/iot-baby-monitor-research.html
4. https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/
5. https://www.iso.org/isoiec-27001-information-security.html
6. https://www.nist.gov/
7. https://telecomindustrydialogue.org
8. http://vodafone.com/content/dam/sustainability/pdfs/telecom_industry_dialogue_ principles.pdf

vodafone.com/iot