5G IoT Device and Platform Testing

QinetiQ 5G Security and Resilience

The adoption by businesses, enterprises and industry of the Internet of Things (IoT) has been driven by the desire to drive process efficiencies and increase productivity; up to 2% potential productivity gains have been reported by some manufacturers using IoT working on a UK 5G testbed.

IoT provides enhanced awareness of critical operations through the collection and analysis of data, allowing smart decision making in an increasingly automated fashion. This move towards the automation of core operational processes introduces a security risk, which is compounded by the fact that many IoT devices will be deployed in the field for in excess of 25 years – for example, in 2017 security flaws were found in a pacemaker controller. This risk has been acknowledged by governments, regulators and standards bodies, with a slew of guidelines, standards and regulations on IoT security – for example, there are now European standards on IoT security issued by ETSI, guidelines from trade bodies such as the mobile industry's GSMA, and consultations on regulation by the UK Government. With 5G becoming the de-facto connectivity technology for IoT, how can developers, providers, and users of enterprise IoT solutions be confident that their 5G IoT solutions are secure?

Leveraging our unique insight and knowledge in the cyber security domain, QinetiQ can assess IoT devices and platforms as part of a comprehensive resilience assessment. Our 5G IoT Device and Platform Testing service provides security testing and assessment of 5G IoT devices and platforms, including software. The service is tailored to your IoT solution and security requirements, to deliver maximum benefit. It allows you to get security right before deployment, and supports you in providing through-life security via upgrades and updates.

Key Features and Benefits

Understand and Mitigate IoT security issues
Comprehensive resilience testing and assessment identifies potential security problems and recommends mitigations, allowing you to stay ahead of the hackers and not become another cyber security statistic.

Independent, trusted and impartial
Our testing is designed and delivered by 5G security experts. We work to, or ahead of, industry best practice. We don't sell security products so are truly independent in the advice we give on how to mitigate issues found.

Dedicated 5G Testing Network
Our dedicated 5G testing network allows us to identify risks in a safe, trusted, managed 5G environment, through the delivery of 5G specific testing.

Holistic approach, tailored to you
Our holistic testing approach considers all aspects of your IoT solution – hardware, software and platform – making sure no system aspect is missed. We tailor our testing to the security needs of your organisation, customers and sector, making it relevant and affordable. Our findings and recommendations, delivered via an easy to read report and face-to-face briefing from our 5G security experts, help you to take concrete actions to improve the resilience of your IoT system.

The service is delivered in two phases:

- **Security Testing Phase** – during this phase the IoT device, software and platform are security tested on our 5G testing network. We first understand your security requirements, determining the importance of confidentiality, integrity and availability to your business in the context of your IoT system. We then tailor our structured sequence of testing to your IoT system and security requirements. Having a dedicated 5G testing network allows us to tailor testing to any IoT device, especially those without a user interface, by monitoring the 5G network traffic directly. Typical testing stages include:
  - Malware scanning – to check for malicious software within your IoT solution. These can often be unintentionally introduced by use of third party libraries;
  - Network end-point analysis – to check where your data is being sent. Many popular libraries can send data outside of your enterprise, for example in the form of crash reports;
  - Behavioural and performance analysis – to check that your IoT system interacts with the network as expected, and does not put unexpected performance demands onto the network;
  - Bespoke testing – testing tailored to your device and requirements. For example we can perform availability testing using interference sources to check how quickly your IoT system recovers from network disruptions.
- **Security Assessment Phase** – during this phase the whole IoT system is decomposed and a security assessment conducted. The security assessment considers the IoT device hardware, its firmware and software, as well as IoT platform software running in the cloud. We use the industry best practice STRIDE framework to perform a threat assessment. This helps you to understand questions such as:
  - Can unauthorised devices access my IoT system?
  - Is the origin of data is checked?
  - Is my data protected from eavesdropping?
  - Is my system resilient to a denial of service attack?
  - Can unauthorised users gain admin or root access to my system?

Once these potential security issues have been identified, they are rated according to your appetite for risk, and mitigations recommended.

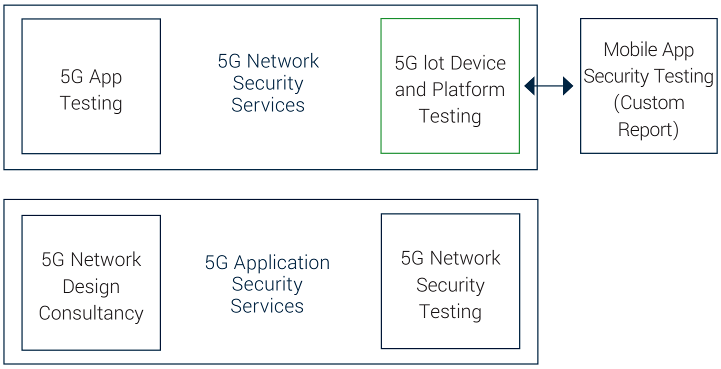
An easy to understand report is delivered at the end of these phases. Our 5G IoT security experts explain the key findings and recommendations to you face-to-face, to assist you in mitigating any issues.

Our IoT Device and Platform Testing can be used at different points in the lifecycle of your IoT project: from early prototype testing during design phases, to iterative testing during the development phase, through to post deployment testing of enhancements and updates. It helps you understand how secure and resilient your IoT solution is (for example how well it protects your data, or how well it recovers from a network disruption), the impact of any short-comings, and practical mitigations to fix these.

QinetiQ 5G Security and Resilience

This 5G IoT device and platform testing service forms part of QinetiQ's wider 5G Security and Resilience portfolio, which provides security and assurance of the 5G network, smartphone applications, and IoT through a suite of integrated consultancy and testing services.
In particular customers may wish to combine this service with:

- **5G App Testing** – find out how secure the 5G smartphone apps you plan to deploy are. Standard or enhanced reports can be purchased on either a one-off or subscription basis. Combine with 5G IoT Device and Platform Testing to give a complete application level testing solution for 5G.
- **5G Network Security Testing** – a comprehensive suite of security assurance testing services for 5G networks. Combine with 5G IoT Device and Platform Testing to give a complete 5G IoT test and assurance solution for the network, IoT platform, and devices.


5G App Testing
5G Network Security Services
5G Iot Device and Platform Testing
Mobile App Security Testing (Custom Report)
5G Network Design Consultancy
5G Application Security Services
5G Network Security Testing

5G IoT Device and Platform Testing forms part of our wider Cyber & Digital Resilience portfolio. It links to the custom report option of QinetiQ's Mobile App Security Testing service, which provides bespoke security testing for smartphone apps across a range of technologies.

Collaborating with QinetiQ

At QinetiQ we bring organisations and people together to provide innovative solutions to real world problems, creating customer advantage.

Working with our partners and customers, we collaborate widely, working in partnership, listening hard and thinking through what customers need. Building trusted partnerships, we are helping customers anticipate and shape future requirements, adding value and future advantage.

www.QinetiQ.com

For further information please contact:

Cody Technology Park
Ively Road, Farnborough
Hampshire, GU14 0LX
United Kingdom

+44 (0)1252 392000
customercontact@QinetiQ.com
www.QinetiQ.com