5G Network Security Testing

QinetiQ 5G Security and Resilience

The introduction of 5G has seen a greater focus on network security and resilience than previous generations. Consumers are demanding higher levels of security and privacy – with trends such as use of Ad-Blockers and anonymised Tor browsing. Enterprises require high levels of availability and protection of business critical data when transitioning critical operations to 5G. Interruptions to 24/7, just-in-time, operations can cause £100,000s of lost revenue.

Moreover, governments are legislating on 5G network security to protect national security interests, as well as the data and privacy of their citizens – for example, the UK's Telecoms Supply Chain Review in 2019 announced legally enforceable Telecoms Security Requirements for Mobile Network Operators (MNOs), and the EU introduced the Network Infrastructure Security Directive in 2018, with fines of up to £17m or 4% of global turnover. All these stakeholders want proof of compliance with security requirements.

The threat to 5G systems is also greater than in previous generations – distributed assets enabled by software based networking present more opportunity to hackers; jamming is now economically viable with low cost radios readily available, and deployment of 5G in industrial settings subjects it to unintentional interference from industrial processes such as welding. How do you prove to yourself, your customers and regulators that your 5G equipment and network are robust and secure – not just on paper, but when deployed and operational?

QinetiQ has developed a comprehensive suite of services for testing the security and resilience of 5G networks, equipment and deployments, to address the needs of mobile network operators, equipment vendors, regulators, and enterprises wanting to deploy 5G.

All of our testing forms a balanced approach to managing risk, based on industry best practice and years of experience in the government and critical national infrastructure sectors. We bring together cyber security, spectrum, radio and 5G expertise and testing experience to offer you specific 5G testing services centred on your needs. Our testing services cover a full range of security testing from pre-deployment EM surveys through to deployed network resilience and penetration testing. The services can be offered separately, or as part of a package, depending on your testing requirements.

Key Features and Benefits

Independent, trusted and impartial – our testing is designed and delivered by accredited security professionals and 5G 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.

End-to-end testing solution – we provide complete end-to-end security testing for 5G networks. This is vital to ensuring there are no gaps in your security.

Prove security compliance and resilience to stakeholders – provides you with the test evidence to prove your 5G network meets the security and resilience demanded by stakeholders, in easy to understand test reports.

Accelerate deployment – as the only provider of dedicated 5G security testing, it is our job to worry about 5G security. We fold-in our cyber security experience from a wide variety of sectors so that you can concentrate on your deployment, whilst being confident about its security.

Radio Interface testing – our unique RF Testing capability allows you to understand your resilience to interference on the radio interface – be this from malicious jamming or unintentional interference from industrial processes. Adopting our suggested mitigations will improve your resilience, reducing network down-time as well as improving service availability and continuity.

QINETIQ

Test your security policies − Information Assurance Testing provides you with an assessment of your organisation's security policies and procedures for your 5G network. It is conducted within a framework based on industry best practice from the UK's National Cyber Security Centre (NCSC), and the Centre for Internet Security (CIS). Our NCSC Certified Professional (CCP) consultants first gather information from security and network documents, and questionnaires, before assessing the network security policies, procedures and measures. The final step is to generate a report of findings and recommendations, which we discuss with you during a face-to-face briefing.

Test for common security issues on your network − Automated Network Testing quickly and easily identifies common security issues on your 5G network using a suite of automated network security tools. Issues such as unpatched and out of date software, weak security implementations (e.g. unencrypted links), poor network addressing, etc., are identified and reported. To minimise disruption, testing is conducted remotely where possible.

Test your resilience against hackers − Penetration Testing puts the resilience of your 5G network security to the test. Our testing is tailored to your needs and delivered by experienced PEN testers who are all CHECK qualified. Testing is focused on the non-radio parts of the network and can either be conducted remotely or at your premises. Coupling this testing with RF testing gives a full resilience test of a 5G network.

Test your resilience against jamming − RF Testing assesses your Radio Access Network (RAN) equipment against passive and active attacks on the radio interface, including resilience to unintentional interference. Testing can either be conducted at your premises, or using our 5G test network. Coupling this testing with PEN testing gives a full resilience test of a 5G network, and with an EM Environment Survey can verify a network's post deployment robustness in a harsh EM environment.

Test your radio environment − EM Environment Survey provides a pre-deployment radio survey to determine if 5G can work in your planned location, and to identify possible interference issues. This is most valuable for 5G networks (including private networks) which will be deployed in noisy EM environments, such as factory production lines. Coupling this survey with onsite RF Testing gives confidence (both pre and post deployment) of your 5G network performance in a harsh EM environment.

QinetiQ 5G Security and Resilience

This 5G network security 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 Network Design Security Consultancy** − a bespoke security consultancy service, specifically focused on 5G, enabling delivery of secure 5G network designs. Combine with 5G Network Security Testing to give confidence in your security from network design through to deployment.
- **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 Network Security Testing to give a complete security testing solution for consumer orientated networks.
- **5G IoT Device and Platform Testing** − a bespoke IoT security testing service. Combine with 5G Network Security Testing to give a complete security testing solution for IoT orientated 5G networks.

5G Network Security Testing also links to a number of services within QinetiQ's wider Cyber and Digital Resilience portfolio, which test the security and resilience of the enterprise, its networks and information infrastructure.
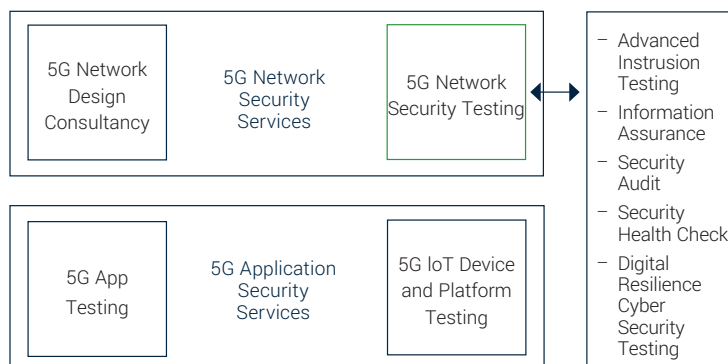
Collaborating with QinetiQ

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