White Paper

5G Security

Reduce Your Risks as You Explore New Opportunities

Introduction

5G is a limitless market opportunity—if you can reduce the risks for end users, your supply chain, and your business. As one recent analyst report reminds us, "Trust is the foundational principle for technology adoption."[1]

Yet trust is an elusive commodity in developing secure 5G use cases. The complexity of 5G security is so overwhelming that it actually creates a new form of risk: inertia. If your business cannot solve the security challenges of 5G, it risks falling behind and incurring the opportunity costs of inaction. At the same time, there is urgent pressure to deploy new services quickly, compounding the risks.

5G network equipment manufacturers and service providers need trusted guidance on how to integrate security into 5G deployments, how to continuously assess the effectiveness of the security they've put in place, and how to focus on innovation rather than risk.

This white paper addresses those issues. It provides an overview of the 5G security challenge, new insights into how to approach 5G security, and specific recommendations for continuously improving the security of 5G infrastructure.

[1] *TIA, 2020.*

Overview of 5G security challenges

The allure of 5G is compelling, with 10-100x peak data rates compared with 4G, 10x decrease in latency, and 100x coverage density compared to 4G.

However, 5G will not be successful without a well-executed security strategy that addresses the wide range of needs across multiple dimensions including:

- **Multiple approaches**, which tend to fall within three broad categories: Prevention, detection, and remediation
- **Multiple elements** and layers to account for, including core, radio access, mobile edge, end-user device, and transport
- **Multiple locations**, including internal networks and devices, remote networks and devices
- **Multiple supply chain considerations**, such as accounting for the security of new suppliers, supplier network access, equipment supply, and user and network data
- **Multiple processes**, from secure operations, monitoring and auditing procedures to secure design, configuration, hardening, and so on
- **Multiple telecom standards** including security protocols, algorithms, interfaces, etc.
- **Multiple criticality levels**, ranging from low-criticality use cases such as games and virtual reality; to mid-level criticality such as consumer-grade IoT and smart grid; to high-criticality use cases such as autonomous vehicles, IIoT, and so on
- **Multiple phases of deployment** ranging from planning, to R&D, to innovation, to actual implementation and ongoing monitoring

In addition, any discussion of 5G security must include consideration of new network and device security threats. These range from threat surfaces such as virtualization (NFVi) attacks and multi-vendor weakness, cloud edge distribution attacks, massive IoT attacks, and security gateway attacks, to ever-evolving attack risks such as data breach, DDoS, resource exhaustion, man-in-the-middle, malware, fraud, VLAN hopping, authentication, authorization, and more.

Four ways to view 5G security

Given the multi-faceted nature of 5G security, what is the best way to begin addressing the challenges? We have seen the emergence of several basic philosophies:

1. **5G is a Pandora's box**, representing a massive security risk as software, network disaggregation, higher volumes of devices and cell sites, an influx of new vendors and open source trends exponentially.
2. **5G is potentially more secure than any previous network** given that 5G harnesses many traditional, tried-and-true network technologies and the underlying architecture is capable of incorporating a number of advanced security mechanisms.
3. **Securing the supply chain is the key**, because 5G is fast becoming an integral part of cross-enterprise and national critical infrastructure.
4. **Spirent's view**: all of the above are accurate, but 5G must be seen first and foremost as a source of competitive advantage and innovation rather than a source of risk, fear, and inertia—because when security is assured, businesses can drive innovation forward with confidence.

The optimal starting point in crafting a 5G security strategy, in our opinion, is to include 5G security in every business conversation from the outset and work with vendors you can trust to deliver security across all categories, particularly across the supply chain.

When you can build security in rather than bolt it on, and when you can test, validate and trust the security measures you put in place, you are capable not only of implementing trustworthy 5G services but also innovating and adding new value continuously.

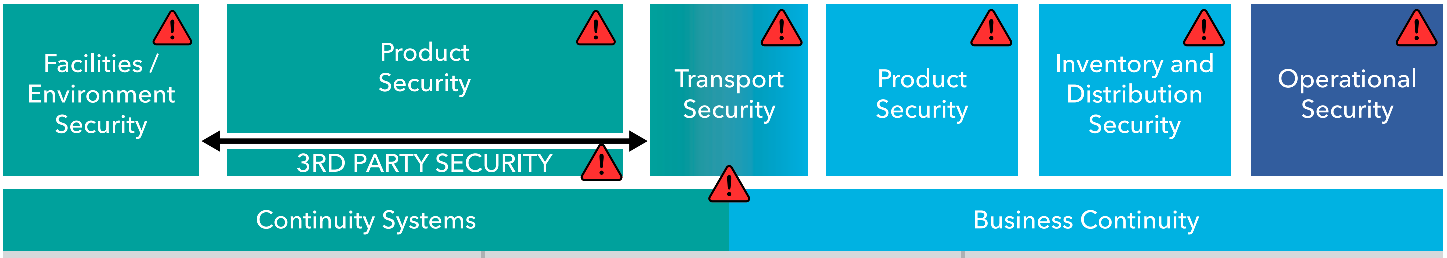
Securing 5G requires securing the supply chain

Recent reports from major analyst firms, government agencies, and technical authorities covering 5G security consistently point to the need to focus 5G security efforts on the supply chain.

The role of suppliers in building and operating 5G networks, the complexity of the interlinkages between suppliers and operators, and the degree of dependency on individual suppliers underscore the need for this approach. More specifically, the rapid growth and diversity of the 5G supply chain introduces a variety of new risks, including (to name just a few):

- ⚠ **Facility/environment security** – Poor or out-of-date security systems and processes such as firewalls, gateways, access control, and so on
- ⚠ **Product security** – Poor or limited security by design, lack of standards compliance, patch and code management
- ⚠ **Third party software** – Limited or poor security compliance
- ⚠ **Continuity systems** – Recovery/mitigation systems out of date, untested or compromised
- ⚠ **Insider risks** – Malicious or inadvertent introduction of vulnerabilities
- ⚠ **Self-policed compliance** – Poor or non-mandatory compliance schemes
- ⚠ **Delays** – Supply chain holdups that impact agility/costs

These and other risks extend across the entire spectrum of interactions among suppliers and service providers, as illustrated in the graphic below.



Supplier

- ⚠ Facility / environment security
- ⚠ Product security
- ⚠ Third party software
- ⚠ Continuity systems
- ⚠ Insider risks

← Transport →

- ⚠ Weak encryption
- ⚠ Poor authentication
- ⚠ Non-approved equipment
- ⚠ Audit log tampering

Service Provider

- ⚠ No revalidation and auditing of supplied product
- ⚠ Lower security policies on inventory and internal distribution
- ⚠ Recovery / mitigation untested or compromised
- ⚠ No continuous security auditing

A wide range of new security challenges have emerged across the 5G supply chain.

On the other side of the coin, new benefits accrue to those who can effectively address the security challenges of the 5G supply chain, including:

Efficiency and agility

- Increased automation and accelerated delivery flows
- Reduced process deviations

Resiliency

- Reduced risk identification and resolution times
- Increased continuity and mitigation measures

Visibility

- Increased auditability/traceability
- Reduced costs/penalties

Trust

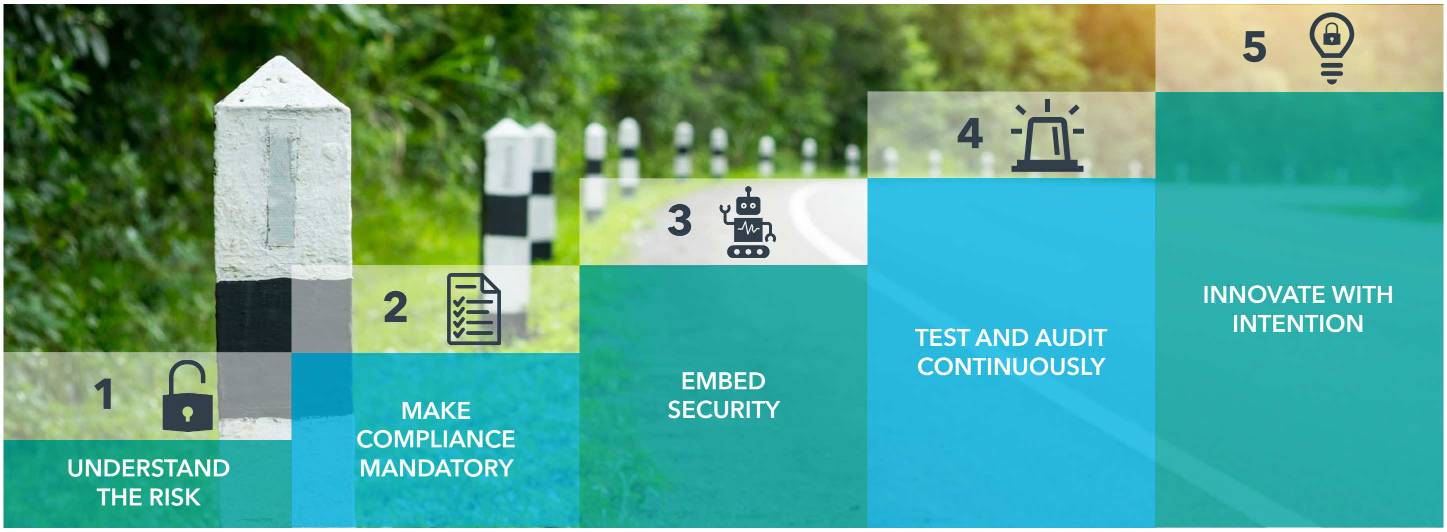
- Increased confidence in suppliers and processes
- Reduced supplier attrition and accelerated onboarding of new suppliers

New opportunities

- Network Slice Isolation for private networks and industry
- Network-based security as a service provided, managed and guaranteed to enterprises
- Active treatment within operational networks to dynamically triage and quarantine risks

Securing and accelerating 5G security initiatives

Delivering on the security demands of 5G is a journey, not a project. There are many milestones along the way. Based on our many years of experience assisting network equipment providers, data communications vendors, and service providers in testing and validating their equipment and networks, Spirent is in a unique position to offer guidance on securing and accelerating your 5G security initiatives while minimizing risk. Our recommendations span understanding the risk, mandating compliance, embedding security, continuously testing and auditing, and innovating with intention.



The journey to 5G security includes these five major milestones.

1. Understand the risk

The first step in 5G risk mitigation is identifying, defining, and quantifying risk scenarios. Spirent recommends that companies begin by testing their environment to identify gaps in 5G security coverage and verify your networks' ability to mitigate risk for 5G device weaknesses. It is important to keep in mind that 5G creates new security risks even for previously trusted equipment, and it is never safe to assume safety without testing. For example, never trust certified devices – they are still the weakest link in 5G security.

In addition to the risk factors already described in this paper, the latest Coordinated Risk Assessment Report from the Network and Information Security (NIS) Cooperation Group, serving the European Union (EU), highlights the following risk categories:[2]

I	**Risk scenarios related to insufficient security measures**	**R1** – Misconfiguration of networks **R2** – Lack of access controls
II	**Risk scenarios related to 5G supply chain**	**R3** – Low product quality **R4** – Dependency on any single supplier within individual networks or lack of diversity on nation-wide basis
III	**Risk scenarios related to modus operandi of main threat actors**	**R5** – State interference through 5G supply chain **R6** – Exploitation of 5G networks by organized crime or organized crime group targeting end-users
IV	**Risk scenarios related to interdependencies between 5G networks and other critical systems**	**R7** – Significant disruption of critical infrastructures or services **R8** – Massive failure of networks due to interruption of electricity supply or other support systems
V	**Risk scenarios related to end user devices**	**R9** – Exploitation of IoT (Internet of Things), handsets or smart devices

2. Make compliance mandatory

It is quickly becoming imperative to ensure that all participants in the 5G supply chain are required to meet all relevant compliance standards. Spirent recommends that in addition to continuously auditing 5G supply chain members, businesses should go deeper and include code audits for back doors and other software risks, and require device suppliers, particularly IoT device suppliers, to be security certified (e.g. CTIA IoT Cybersecurity certification).

[2] *"Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures," NIS Cooperation Group, 2020*

3. Embed security

When you embed security into your 5G deployments now, security can become a competitive advantage later – because you can deploy, refine, and innovate on your 5G services with confidence that your users, your business, and your supply chain will remain safe. Key recommendations include:

- **Assess your strategy** for securing 5G services based on their specific goals, capabilities, and timelines, and ensure that security is an integral part of every discussion of your 5G plans and initiatives.
- **Embed security** into key processes from the outset, thereby improving their ability to meet compliance requirements, increase productivity, accelerate time-to-market for new innovations, cut costs, and reduce risks.
- **Encrypt all traffic**/data inflight and at rest, enabling you to continuously audit security policies and access control to ensure that they are working and remain fit for purpose.

4. Continuously test and audit

One advantage of 5G networks is that they are dynamically configurable; however, traditional penetration testing will not be able to keep pace with 5G network evolution, and existing vulnerability assessment and asset management tools are not designed for dynamic environments.

Moreover, traditional point-in-time assessments alone are not frequent enough to provide a true vision of the threat landscape in 5G networks. The move to 5G is the right time to implement continuous and thorough assessment of the environment using up-to-date threat intelligence. For example, we recommend that companies do the following:

- Continuously validate your 5G infrastructure and vendor software security.
- Continuously validate your suppliers and supply chain security to verify that it is still fit for purpose. Security revalidation must be as agile and continuous as the volume of releases coming into the network.
- Continuously assess your networks and devices in the operational domain to proactively identify risk and handle mitigation. Active monitoring (i.e. synthetic attack traffic generation) and analytics will be extremely helpful in this area.
- Continuously assess applications, APIs, authentication mechanisms, and container orchestration for known vulnerabilities, security misconfigurations, and access control.
- Validate the security efficacy of the supporting PKI (public key infrastructure) platform that would be issuing the certification, check certificate strengths, supported cypher suites, key length, secure key storage, certificate lifecycle management, connections between network functions using TLS (VNF, CNF and PNF) and PKI security requirements compliance.
- Continuously war-game your network to discover weaknesses and future risks.
- Automate all testing, auditing, and validation processes where possible.

5. Innovate with intention

Innovating with intention means taking responsible risks based on actionable intelligence to speed up innovation. We recommend the following actions to enable this capability:

- **Minimize the risks of innovation** by gathering the intelligence needed to identify, quantify, and respond to security risks, compliance risks, and business risks before they impact the live production environment. Assured that security is always being addressed, businesses can focus on creating the right 5G features and functionality—and innovate with intention.
- **Leverage ideas from everywhere**. Taking a community-oriented approach to innovation arms the organization with the resources and agility to react quickly to changing market dynamics. Use analytics to proactively identify, quantify, and respond to security risks, compliance risks, and business risks.

Spirent solutions: foundation of trust

Spirent Communications is uniquely qualified to assist with 5G security planning, testing, auditing, and validation—across the 5G supply chain. We have been a trusted advisor to the ICT industry for decades, testing and validating the equipment modern networks depend on; we bring a vendor-neutral approach to testing and validation; our security and telecom domain experts are trusted by global telecom CSPs and suppliers; and we are a trusted supplier and advisor to government agencies worldwide.

Spirent's industry security accreditations include CREST, Cyber Essentials, OSCP, ISO, GXPN, and more. In addition, Spirent actively supports and contributes to industry standards such as CTIA IoT Cybersecurity, and we are a founding member of NetSecOPEN, the first industry organization focused on the creation of open security performance testing standards. By supporting these community-based approaches to standards, we not only continue our tradition of innovating with intention but enable our customers to do so as well.

Trusted Advisor

- Vendor **neutral** partner
- Seasoned **security** & **telecom** experts
- Used by **worldwide** telecom suppliers and CSPs
- Trusted supplier/advisor to **Government**

Industry Recognized

ctia Authorized™ Test Lab

CREST

C|EH Certified Ethical Hacker

ISO 27001 Certified — Information Security Management System

GXPN

OFFENSIVE security OSCP

CISCO CERTIFIED CCENT NETWORK

CISSP®

NetSecOPEN
Open standards in security product testing

Leading Lights AWARDS 2019 WINNER

2019 Test and Measurement Vendor for 5G

#1 in 5G Core / NFV and High-Speed Ethernet Test and Validation

Innovative Solutions

securitylabs
Test services

cyberflood
Automated test tools

Data Breach Assessment
Continuous assessments

Test as a Service
Continuous supplier validation

- **Realistically test** security performance and efficacy
- **Certify** suppliers and supply chains
- **Continuously** assess and audit security
- **War game** future risks and mitigations

Spirent recognizes that a new breed of Security Test and Assurance is required that can seamlessly and continuously operate across the lifecyle as solutions are developed, deployed, operated, and transitioned through digital supply chains.

Our security focus is prioritized towards three key areas:

1. Realistically testing security performance and efficacy to reduce risks and costs.
2. Certifying suppliers and supply chains to enhance efficiency and build trust.
3. Continuously assessing and auditing security in both the lab and live networks to harden resilience and reduce compromises.

About Spirent Communications

Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks.

We help bring clarity to increasingly complex technological and business challenges.

Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled.

For more information, visit:
www.spirent.com

AMERICAS 1-800-SPIRENT
+1-800-774-7368
sales@spirent.com

EUROPE AND THE MIDDLE EAST
+44 (0) 1293 767979
emeainfo@spirent.com

ASIA AND THE PACIFIC
+86-10-8518-2539
salesasia@spirent.com

To meet these priorities, Spirent offers a broad range of capabilities and solutions that facilitate 5G security testing, auditing, supplier certification, and validation, including:

Continuous Assessment and Validation solutions such as:

- **VisionWorks**: a rugged virtual test platform that emulates realistic user activity to proactively test 5G networks and services.
- **CyberFlood Data Breach Assessment**: delivers accurate, automated, continuous and thorough assessment of live 5G production network environments, using an always-up-to-date database of hyper-realistic attack, malware, data loss prevention, and applications scenarios.

Automated test tools and emulators including:

- **CyberFlood**: a testing platform that generates realistic application traffic and attacks to test the performance, scalability and security of 5G infrastructures.
- **5G Digital Twin**: a new agile, automated approach to testing and assurance providing an emulated, software replica of the 5G physical network.

Consultancy and test services including:

- **SecurityLabs**: provides comprehensive scanning, penetration testing, and monitoring of 5G networks, applications, devices and endpoints; or our consultants can ensure that your teams have the right skill sets and tools to perform those tasks on their own.
- **Test-as-a-Service**: offers continuous supplier validation as a managed service and allows you to war-game future risks and mitigations.

Spirent provides end-to-end capabilities across all dimensions of the 5G security challenge, including security across the 5G supply chain. We facilitate 5G supply chain continuity planning, researching, and prototyping, including investigation of disaster recovery (DR) scenarios, rapid vendor quarantine and displacement using 5G functional disaggregation and slices to create isolated treatment centers, and more.

The result: Spirent enables customers to implement comprehensive risk reduction as they explore the opportunities of 5G adoption.

Contact us and learn more.

Please contact us for additional information about Spirent's capabilities in 5G security or visit our website at [URL]. We would be pleased to discuss your particular requirements, arrange a demo, and provide complete information about our services and solutions.

spirent™
Promise. Assured.