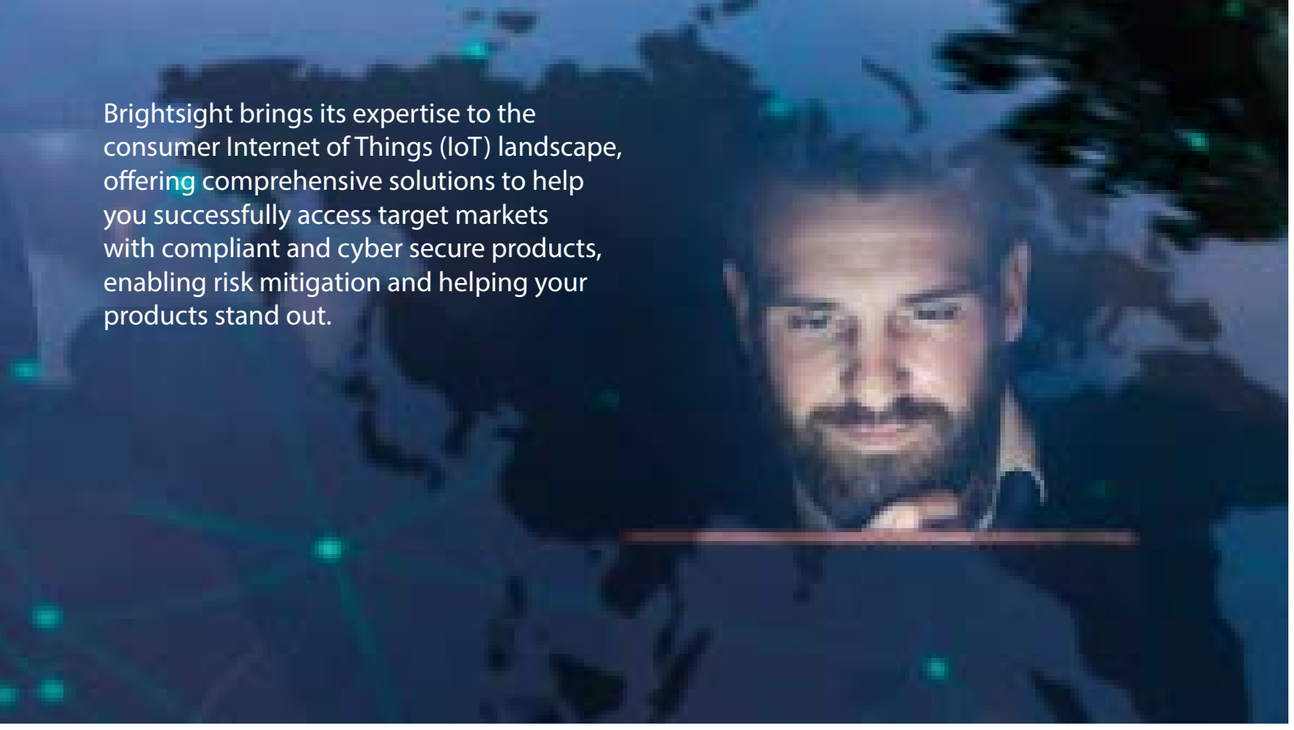
Brightsight cybersecurity evaluation services for consumer IoT

DELIVERING SECURE CONNECTED PRODUCTS
TO GLOBAL MARKETS

brightsight

By SGS



Brightsight brings its expertise to the consumer Internet of Things (IoT) landscape, offering comprehensive solutions to help you successfully access target markets with compliant and cyber secure products, enabling risk mitigation and helping your products stand out.

Introduction

In our increasingly interconnected world, where cyber threats are on the rise, cybersecurity has never been more critical. A state-of-the-art third-party security evaluation provides both users and developers with the assurance that their solutions are secure.

SETTING THE SCENE

The IoT is the extension of internet connectivity into physical devices through electronics, software, sensors and actuators that enable interaction and data exchange.

This ‘smart’ technology is all around us, in our televisions, speakers, appliances, locks, exercise trackers and even the games we play that connect us to opponents all over the world.The IoT has many advantages, but inherent vulnerabilities mean suppliers must find ways to protect data and safeguard financial, medical, automotive, industrial and consumer systems at all times.

MARKET DRIVERS

COMPLIANCE

Does your product conform to recognized standards for security and performance?

RISK MANAGEMENT

Has due diligence been performed during development and manufacture?

MARKET DIFFERENTIATION

Can you demonstrate your product is safer and more secure than those of your competitors?

Consumer IoT regulatory landscape

As the number of connected devices explodes exponentially, privacy and security concerns for connected products have become increasingly important topics. Competent authorities around the world have published various cybersecurity regulations, including the EU Cybersecurity Act, the EU General Data Protection Regulation, the California Consumer Privacy Act, the EU Radio Equipment Directive (RED) and the UK Product Security and Telecommunications Infrastructure (PSTI) regulation.

In the rapidly evolving security landscape, regulations are beginning to require more and more evidence of cybersecurity management in IoT – e.g. the EU’s Radio Equipment Directive (RED) Article 3.3 (d,e,f) and Cyber Resilience Act (CRA), the Singapore Cybersecurity Labelling Scheme (CLS), the U.S. Cyber Trust Mark, the UK’s Product Security and Telecommunications Infrastructure (PSTI) regulation and other internationally recognized standards, including ETSI EN 303 645, NIST IR 8259A, NIST IR 8425, IEC 62443-4-2 and ISO 21434.

EU RED CYBERSECURITY

The European Commission (EC) has taken measures to strengthen the cybersecurity of wireless devices and products available in the EU by adopting a delegated act under the RED. The cybersecurity provisions outlined in RED Article 3.3 cover (d) networks, (e) personal data and privacy, and (f) protection from fraud. These apply to devices capable of communicating via the internet, including toys and childcare equipment, and wearables. Starting from August 1, 2025, all wireless devices and products sold in the EU will be required to comply with the RED delegated act.

EU CRA

This is the first EU-wide legislation introducing common cybersecurity requirements for manufacturers and developers of products with digital elements, covering both hardware and software. It is expected to come into force in the third quarter of 2024 and will be mandatory after three years.

SINGAPORE CLS

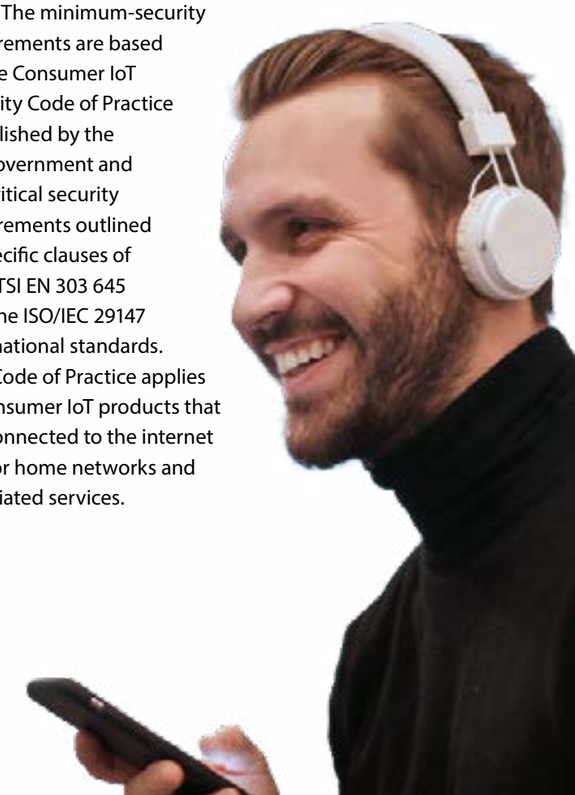
The CLS for Singapore is voluntary for most consumer products, but mandatory for routers. It is based on ETSI EN 303 645 and the Infocomm Media Development Authority’s (IMDA) IoT cyber security guide, and offers four levels of assurance.

US CYBER TRUST MARK

The U.S. Cyber Trust Mark is a voluntary labeling program based on specific criteria published by the National Institute of Standards and Technology (NIST) relating to passwords, data protection, software updates and incident detection capabilities.

UK PSTI

The UK PSTI regulations mandate security requirements which will apply from April 29, 2024. The minimum-security requirements are based on the Consumer IoT Security Code of Practice established by the UK Government and the critical security requirements outlined in specific clauses of the ETSI EN 303 645 and the ISO/IEC 29147 international standards. This Code of Practice applies to consumer IoT products that are connected to the internet and/or home networks and associated services.



Our services

Our services include training, pre-assessment, evaluations, certification(s) and post-evaluation maintenance. Through our global network, we can assess all products against a wide variety of internationally recognized standards, and as a Notified Body, we can issue EU-type certification for products destined for European markets, to show compliance with RED 3.3 (d), (e), (f).

PRE-EVALUATION

- Training/workshop
- Evidence readiness
- Product design review
- Pre-assessment
- Developer advisory support

SECURITY EVALUATION

- ETSI EN 303 645
- ETSI TS 103 732 (CMD PP & MDSCert Annex)
- NIST IR 8259A
- NIST IR 8425
- UK PSTI
- RED article 3.3 (d),(e),(f)
- Platform Security Architecture (PSA) Certified
- Security Evaluation Standard for IoT Platforms (SESIP)

POST-EVALUATION

- Continuous monitoring
- Continuous conformance
- Certification health check

SGS Cybersecurity Mark

Upon successful evaluation, compliant products can then carry the internationally recognized SGS Cybersecurity Mark, demonstrating to customers the adoption of best practice and product conformity to defined standards. Our strategic, step-by-step approach to cybersecurity also lets manufacturers benefit from certification against multiple standards in one evaluation.

Transparency for your end consumers via a QR code

Demonstrate compliance for your IoT product

Risk management via a third-party evaluation

Market differentiation with SGS brand recognition

Continuous monitoring of your product's security

We provide comprehensive solutions to support manufacturers in the delivery of compliant IoT products to regulated markets.

Why choose Brightsight as your security laboratory?

With over 40 years of experience in cybersecurity and a growing global network of specialist testing facilities, we are the world's number one security evaluation service provider with over 700 security evaluations completed every year.

We understand the market and the technical requirements relevant to your component or device.

Our dedicated team of security experts supports the streamlining of evaluation criteria into a single assessment process that incorporates all relevant global, regional and vendor requirements

– one evaluation, multiple certifications.

Our numbers

10
Locations around the globe

50+
Security standards and schemes recognitions

40
Years of experience in security evaluations

250+
Security evaluation experts

700+
Security projects performed each year

brightsight
By SGS

We are your first choice for independent testing and developer support services

When you want to efficiently deliver safe and compliant IoT devices to global markets.

- UK PSTI
- ETSI EN 303 645
- ETSI TS 103 732
- RED Article 3.3 (d), (e), (f)
- NIST IR 8259A
- NIST 8425
- Common Criteria
- SESIP
- PSA Certified

When you need to be sure

SGS Brightsight
Brassersplein 2
2612CT Delft
The Netherlands

+31 (0)15 269 2500

brs.iot@sgs.com

brightsight.com