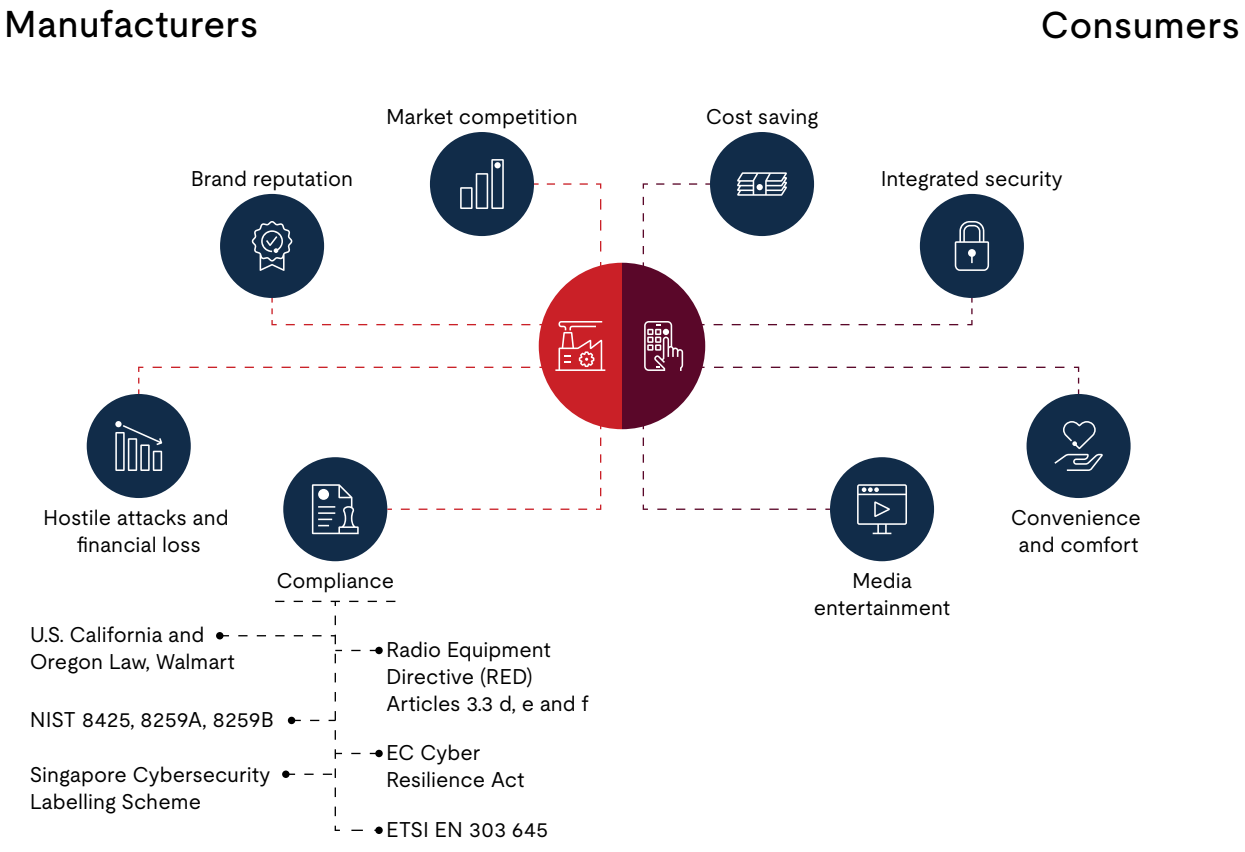
Consumer IoT cybersecurity

Building trust and security in connected consumer products

As consumers increasingly rely on connected Internet of Things (IoT) devices, from locks and baby monitors to connected appliances, they need to be able to trust that these devices are designed, built and managed over their lifetime with security and privacy in mind. According to IPSOS Research, U.K. consumer sales of smart devices have increased 49% since the start of the COVID-19 pandemic. Yet today, many remain vulnerable to cybersecurity threats, as evidenced by reports of cyberattacks scrolling across news tickers around the world. These cyber breaches are made possible by software vulnerabilities that provide entry points of attack. These vulnerabilities put the privacy and personal data of consumers at risk.

Consumer cybersecurity trends and challenges



Collaborate with UL Solutions

Your cybersecurity journey along the consumer product development life cycle

01 Advisory
- Understanding the consumer cybersecurity landscape

02 Training
- Understanding regulatory and standard requirements

03 Gap analysis
- Identifying cybersecurity risks and gaps
- Mitigating risks and gaps by strengthening cybersecurity posture

04 Certification
- Achieving regulatory approval and market access

05 Life cycle management
- Maintaining secure operations during the entire life cycle

Time to market | **Benchmarking** | **Brand protection** | **Risk and cost control**

Consumer cybersecurity solutions

- Help understand and mitigate the unique risks associated with consumer IoT.
- Identify gaps and deploy a risk-based cybersecurity approach as an integral part of business strategy and operations.

I want to differentiate our product in the marketplace based on security.

UL Verified IoT Device Security Rating — Offers a tiered product security verification solution, which is driven by baseline security practices, and results in a differentiated product security label.

Help manufacturers and developers improve the security posture of their solutions by leveraging proven security best practices.

Rate the security posture of IoT products in order to make security more transparent and accessible to consumers.

IoT Device Security Rating

Manufacturers can place the UL Verified Mark on the product, product packaging or on promotional materials in the physical store or online retail environment.

Aligns with global industry recommendations, guidelines and standards:

- ETSI EN 303 645
- Radio Equipment Directive (RED)
- NIST 8259A
- DesignLight Consortium (DLC)
- Many others, including California and Oregon laws

I want to expand my product team's cybersecurity knowledge.

Consumer Device IoT Masterclass — Training course created with the goal of helping IoT device manufacturers and other interested stakeholders understand the basics of consumer device IoT security.

Key principles and philosophy of IoT device security.

Common IoT security best practices, based on relevant global requirements and standards.

Evaluation process – timelines, common issues, and how security laboratories evaluate each requirement.

Consumer Device IoT Masterclass

How consumer device IoT fits into the wider connected world.

Consumer IoT ecosystem and landscape.

Readily adaptable to add optional modules or training variations, including:

- ETSI EN 303 645
- DLC technical requirements
- Impact of the European Commission's Radio Equipment Directive (RED)

I am new to cybersecurity.

IoT Jumpstart Program — Collection of activities and services intended for customers with little or no experience in IoT security who want to gain a basic understanding of the steps they need to take to evaluate their IoT products for compliance.

Provide feedback, answer questions and/or review documents created by you based on our templates to confirm that the documents capture the relevant information.

Provide checklist of security documents and processes required to pass an IoT security evaluation.

IoT Jumpstart Program

Reviewing any existing or in-development security documents and processes related to IoT.

Perform a final gap analysis based on your intended IoT security evaluation (e.g., UL Verified IoT Device Security Rating program, DesignLights Consortium (DLC) or ETSI EN 303 645) once documents have been completed and processes have been documented to give a clear view of what actions must be conducted in order to evaluate whether your IoT devices will be compliant with security requirements.

Why UL Solutions for cybersecurity?

- Independent, trusted third party
- Full life cycle solutions
- Hardware- and software-based security evaluations
- Assessment of security development practices
- Cybersecurity expertise
- Industry knowledge
- Cybersecurity and safety
- Global teams and local support

Cybersecurity foundation

- Expertise in global standards and frameworks
- Extensive knowledge of best practices
- Growing list of Internet of Things (IoT) security solutions

Learn more and speak to one of our experts today at UL.com/ConsumerIoT.

UL Solutions

UL.com/Solutions

© 2023 UL LLC. All rights reserved.

IMS23CS705800
054.02.0323.EN.CYB