UL Global Cybersecurity Services & Standards

Cybersecurity Assurance Program (CAP) for network-connectable products & systems addresses security concerns

As cyber attacks become more sophisticated, harder to protect against, and more costly than ever, security precautions are critical. It is estimated that by 2018, 66% of networks will have an IoT security breach*. Customers worldwide are asking UL to help support their organizations bring safer and more secure products and systems to market. Purchasers would like to address security in their supply chain by having an independent trusted third party, like UL, perform assessments on connected products and on the vendors that manufacture, install, operate and maintain those products.

UL Cybersecurity Assurance Program (UL CAP)

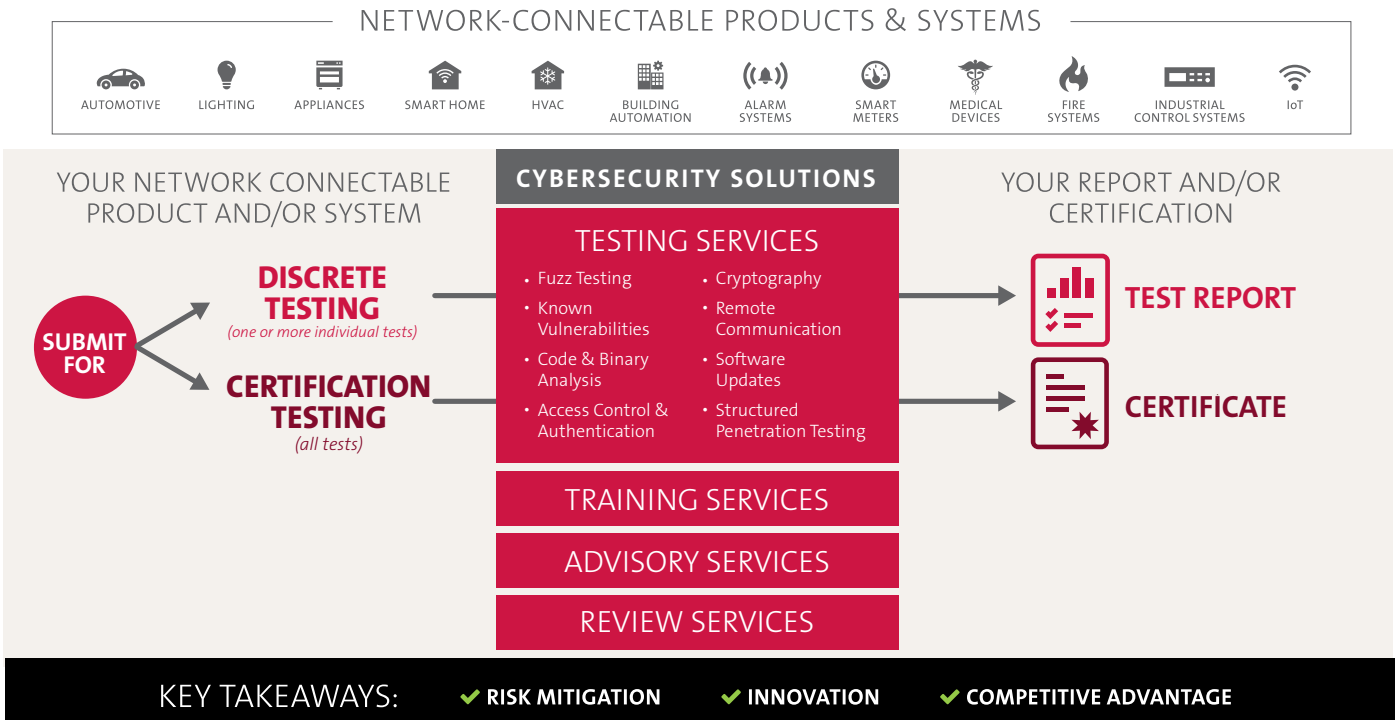
UL helps mitigate safety and performance risks inherent in technologies comprising the Internet of Things (IoT) with the UL Cybersecurity Assurance Program (UL CAP). Using the UL 2900 series of cybersecurity standards, we offer testable cybersecurity criteria for network-connectable products and systems to assess software vulnerabilities and weaknesses, minimize exploitation, address known malware, review security controls and increase security awareness. The UL CAP helps identify security risks in products and systems and suggests methods for mitigating those risks in a wide range of industry functions: industrial control systems, medical devices, automotive, HVAC, lighting, smart home, appliances, alarm systems, fire systems, building automation, smart meters, network equipment, and consumer electronics.

UL cybersecurity services for network-connectable products and systems include:

- Testing security criteria based on UL 2900 cybersecurity standards or custom requirements
- Testing leading to certification based on UL 2900 cybersecurity standards
- Evaluation and risk assessment of vendor processes for developing and maintaining security products and systems
- Training in security readiness for product design and sourcing third party components

For more information, call 1-877-UL-HELPS, e-mail: ULCyber@ul.com or visit www.ul.com/cybersecurity

UL CAP offers trusted third party support with the ability to evaluate both the security of network-connectable products and systems as well as the vendor processes for developing and maintaining products and systems with a security focus. The program allows vendors to concentrate on product innovation with emerging technologies and capabilities to meet the ongoing needs of the marketplace. For increased flexibility, vendors can select the UL CAP services best suited for their current needs.

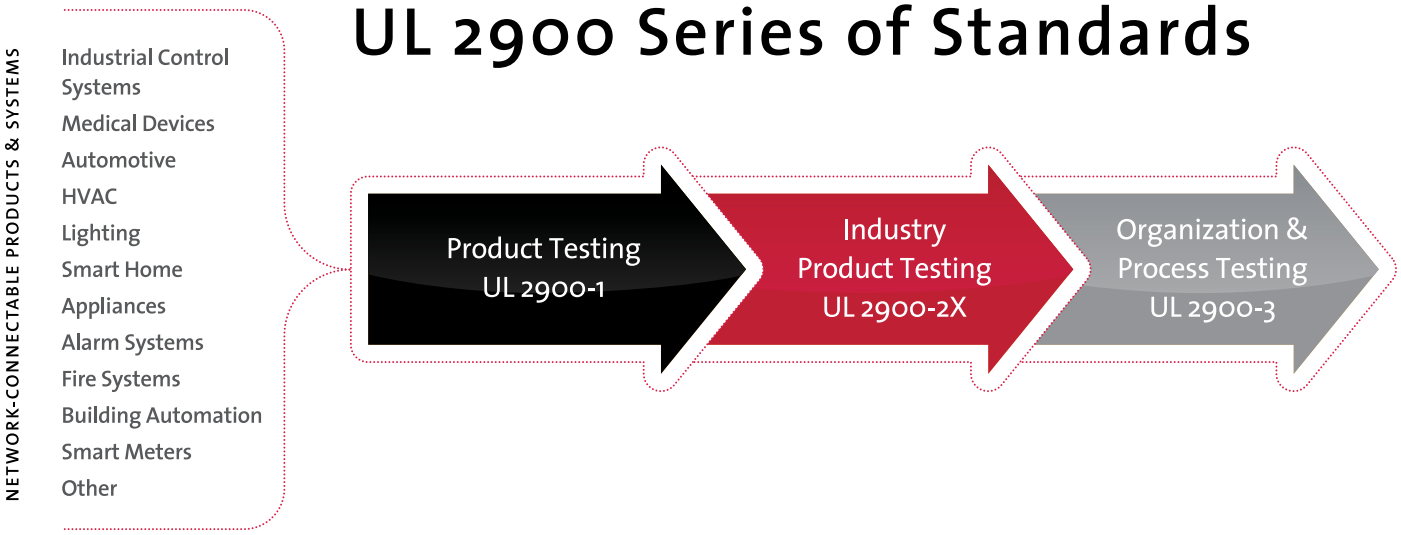


UL 2900 - Cybersecurity Series of Standards

The UL 2900 series of standards has the ability to test and evaluate based on the following criteria:

- **Fuzz testing** of products to identify zero day vulnerabilities over all interfaces
- Evaluation of **known vulnerabilities** on products that have not been patched using the Common Vulnerability Enumerations (CVE) scheme
- Identification of **known malware** on products
- **Static source code** analysis for software weaknesses identified by Common Weakness Enumerations (CWE)
- **Static binary analysis** for software weaknesses identified by Common Weakness Enumerations (CWE), open source software and third party libraries
- Specific **security controls** identified for use in products that reduce the security risk associated with:
  - Access control and authentication on products
  - Cryptography used in products
  - Remote communications to products
  - Software updates on products
  - Decommissioning of products
- **Structured penetration testing** of products based on flaws identified in other tests
- **Risk assessment** of product security mitigation designed into products

UL 2900 Series of Standards



The organizational assessment in UL 2900 will support the evaluation of a vendor, system integrator, or asset owner process for design, development and maintenance of secure products and systems. UL 2900 will continue to evolve to incorporate additional technical criteria as the security needs in the marketplace mature.

Product Testing Deliverables

Meeting the requirements outlined in the UL 2900 series of standards allows a product or system to be certified by UL as "UL 2900 compliant" receiving a certificate and a detailed test report. Additionally, testing security criteria based on requirements in UL 2900 or customer specified requirements receive a test report.

Why Choose UL?

The UL CAP was developed with input from major stakeholders representing the U.S. Federal government, academia and industry to elevate the security measures deployed in the critical infrastructure supply chain. In fact, the UL CAP security efforts are recognized within the U.S. White House Cybersecurity National Action Plan (CNAP) as a way to test and certify network-connectable devices within the IoT supply chain. Additionally, the U.S. Department of Health & Human Services has selected Anura Fernando, Principal Engineer of Medical Software & Systems Interoperability at UL, as a member of the Healthcare Industry Cybersecurity Task Force which was created to identify opportunities for enhancing information security in the Healthcare and Public Health Sector.

Early adoption of the UL CAP provides a competitive advantage in the marketplace and can help with mitigating risk including:

- Unplanned downtime and loss of production
- Costly harm to assets
- Reputational damage

*Source: IDC Research, Inc.

For more information, call 1-877-UL-HELPS, e-mail: ULCyber@ul.com or visit www.ul.com/cybersecurity

100.03.0716.EN.UL