



# SafeCyber™ Digital Security Platform

A suite of digital security solutions designed for connected products

## Democratizing IoT security and empowering connected product stakeholders

Device manufacturers, suppliers, system integrators and other stakeholders from chip to cloud continue to face cybersecurity challenges in today's highly connected world. Product performance and security are at the top of their minds, and navigating through compliance complexity can be a challenging task.

- As they face competitive innovation cycles, how can they release new products faster while still guaranteeing security and compliance with industry regulations?
- How can they evaluate where they stand in terms of product security practices?
- How can they identify the actions they need to take, including process improvements, security techniques and security mechanisms?

As more stringent government and industry cybersecurity regulations emerge across industries, UL understands these challenges and continues to support connected device stakeholders. SafeCyber™, a security and compliance posture management platform, hosts a suite of digitally enabled cybersecurity solutions for connected products to help stakeholders address their cybersecurity challenges.

## Are SafeCyber™ solutions for you?

Product security and development teams at device manufacturers, suppliers and system integrators utilize SafeCyber™ to help improve and enhance their connected devices' security posture across the entire life cycle. SafeCyber™ aims to help you speed up time to market and demonstrate compliance.

As a security posture management platform across verticals, SafeCyber™ hosts a suite of digital security solutions including Maturity Path, Firmware Check and Field Monitoring. Leveraging these solutions, customers can look at security governance and processes as well as apply security to manage and reduce product security risks.



## Maturity Path

Assessing your product security program's maturity and setting the right direction

SafeCyber's Maturity Path provides a security development life cycle maturity assessment for connected devices to help companies enable consistent security across governance and processes throughout product lines. With this holistic overview and analysis, companies can better manage risks and minimize vulnerabilities.

## Firmware Check

Performing a security and compliance check on your device firmware implementations

Firmware Check provides device manufacturers, suppliers and system integrators a security check on their firmware implementations under development, offering a report with elements such as:

- Software Composition Analysis (SCA) and Software Bill of Materials (SBOM) generation
- Known vulnerabilities/common vulnerabilities and exposures (CVEs)
- Unknown vulnerabilities (zero-day vulnerabilities)
- Compliance analysis with several supported standards and guidelines across verticals, including UL's Internet of Things (IoT) Security Rating, ETSI 303 645, ISO 21434, IEC 62443 4-2 and more

## Field Monitoring

Monitoring your firmware security and ensuring continuous compliance

Field Monitoring allows device manufacturers, suppliers and system integrators developing firmware to perform a security check on firmware in the field, providing a report with elements such as:

- SCA and SBOM generation
- Known vulnerabilities/CVEs
- Unknown vulnerabilities (zero-day vulnerabilities)
- Compliance analysis with several supported standards and guidelines, including UL's IoT Security Rating; ETSI 303 645; ISO 21434; IEC 62443 4-2; UL 2900 2-1, the Standard for Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems; and more

## SafeCyber™ key benefits

- Obtain your security governance and processes standing for all your product lines in one integrated digital solution.

- Communicate your security maturity level easily with internal and external stakeholders.
- Speed up firmware development turnaround time while addressing vulnerabilities to help ensure security and compliance readiness.

- Achieve clarity on where you stand and what you can improve on.

UL has extensive expertise in cybersecurity with a global IoT network and Operational Technology (OT) security laboratories, as well as security experts and advisers with specialized knowledge in global security standards, frameworks and best practices. We are committed to helping the industry innovate with new technologies and bring secure products to the marketplace.

For more information about SafeCyber™, visit [UL.com/SafeCyber](https://UL.com/SafeCyber).



Empowering Trust®