



SafeCyber Firmware Check Solution

Perform a security and compliance check on your device firmware implementations

About SafeCyber

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.

Hackers frequently target hardware and firmware within all types of connected devices as they often lack protection. Moreover, firmware vulnerabilities are common and challenging to manage across industries such as healthcare, automotive, industry 4.0 and consumer electronics. Once exploited, they allow hackers to gain access to a company's network and proceed with ransomware attacks, among other threats.

- 83% of businesses experienced a firmware attack in the past two years. ([Microsoft](#))
- 90% of organizations that use operational technology (OT) solutions fell victim to a cyberattack in the two years prior. ([Ponemon Institute](#))
- A single medical device recall can cost up to \$600 million. ([McKinsey](#))
- A global automaker recalled approximately 1.4 million cars in 2015 in one of the first cases involving automotive cybersecurity risks. The recall's impact was significant at almost \$600 million. ([McKinsey](#))

During the development phase, firmware analysis and vulnerability detection can help connected device stakeholders prevent attacks and speed up security and compliance checks for faster time to market.

Perform a security and compliance check on your device firmware implementations with Firmware Check

Firmware Check offers device manufacturers, suppliers and system integrators a security check on their firmware implementations under development, providing 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



UL's Firmware Check offers three service plans, with the option to purchase one, four or 12 scans, based on your needs.

Standard	Pro	Premium
SCA and SBOM	SCA and SBOM	SCA and SBOM
CVEs	CVEs	CVEs
	Zero-day vulnerabilities or compliance analysis	Zero-day vulnerabilities
		Compliance analysis

Is Firmware Check for you?

Firmware Check is for product security and development teams at device manufacturers, suppliers and system integrators developing connected products and looking to speed up firmware development turnaround time while addressing vulnerabilities and advancing security and compliance readiness with the latest standards and regulations. The solution applies to the automotive, healthcare, manufacturing and consumer IoT industries.

What is the process?

Product security and development teams can self-register on the SafeCyber platform and choose a plan with features based on their needs.

- Create an account through www.UL.com/FirmwareCheck.
- Start a Firmware Check project and choose one, four or 12 firmware scans.
- Upload the provided order form with your chosen features and the firmware binary file(s) to scan.
- Upon processing the order, receive your report.

Firmware Check key benefits

- Detect known and unknown vulnerabilities as you develop your firmware for faster remediation.
- Obtain a compliance readiness analysis on industry-leading standards, including ETSI 303 645 and ISO 21434.
- Easily generate a software bill of materials.
- Gain clarity on where you stand and what you need to improve on.

UL has extensive expertise in cybersecurity with a global network of IoT and 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 and to register for a complimentary account, visit www.UL.com/FirmwareCheck.



Empowering Trust®