SafeCyber Field Monitoring Solution

Protect your connected devices in the field with firmware monitoring

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)

In the operational phase, firmware vulnerability monitoring can help connected device stakeholders prevent attacks and maintain their devices' security postures by tracking and remediating vulnerabilities as they come.

Field Monitoring helps ensure your firmware security's continuous compliance

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

- Software Composition Analysis (SCA) and Software Bill of Materials (SBOM)
- Known vulnerabilities/Common Vulnerabilities and Exposures (CVEs)
- Unknown vulnerabilities (zero-day vulnerabilities)
- Compliance analysis with several supported standards and guidelines, including UL's Internet of Things (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.

Our Field Monitoring solution 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

Who is Field Monitoring for?

Field Monitoring is for product security and development teams at device manufacturers, suppliers and system integrators releasing connected products into the market and looking to achieve continuous security by monitoring vulnerabilities and addressing them as they emerge. 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/FieldMonitoring.
- Start a Field Monitoring project on the application 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.
- Define actions for the latest vulnerability report you received through the application.

Field Monitoring key benefits

- Detect known and unknown vulnerabilities for your device firmware implementations in the field for faster remediation.
- Obtain a continuous compliance analysis on industry-leading standards, including ETSI 303 645 and ISO 21434.
- Easily generate an SBOM.
- Gain clarity on where you stand and what you need to remediate to prevent future attacks.

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/FieldMonitoring.

Empowering Trust®