# Solution Brief

## The antidote to reducing medical device cyber risks

IriusRisk

# Key Challenges

As medical devices come on the market with ever greater technical advances, the risk of cybercrime grows, fuelling ransomware attacks on hospitals and healthcare systems, putting patients at medical risk, and leaving device manufacturers facing huge bills.

Digital transformation means patients use increasingly sophisticated devices connected to the cloud containing personal and sensitive data.

But according to a recent report*, 53% of connected medical equipment and other IoMT devices in hospitals have known critical vulnerabilities. Further, nearly a third of bedside IoT devices are at critical risk.

For manufacturers, cyber-attacks have far-reaching consequences. It's not just potential fines and compensation to account for (plus the sizable cost of investigating and patching), there's potential for corporate reputational damage from which it might be difficult to recover. The challenge for medical device manufacturers is to have failsafe cyber security before healthcare professionals, and patients get their hands on the equipment.

**22.5 million healthcare records** were breached in the US in the first half of 2022


of medical devices are at the **end of their life** using older, more exploitable tech


of healthcare IT professionals worry that patient information is **exposed, lost, accessed, or stolen**

*2022 State of Healthcare IoT Device Security Report by Cynerio

Traditionally, finding and eliminating security flaws during medical device software development is costly and time-consuming. The required expertise is hard to find and holds up what should otherwise be an agile development flow.

And while Infrastructure as Code (IaC) overcomes many challenges while creating cloud-based services, your DevOps knows it cannot guarantee secure environments.
Until now.

## Solution Overview

Imagine an easy-to-use threat modeling system that works for your teams throughout the development lifecycle. IriusRisk's incredibly successful platform does this in a way that encourages collaboration throughout the dev process.

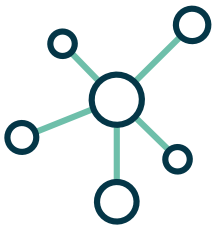
While your teams concentrate on creating impactful software, our automated threat modeling platform works 24/7, constantly assessing risks and evolving threats and vulnerabilities, studiously assessing each IaC definition.

Your teams can generate automated threat modeling of all cloud-native designs from IaC descriptors, including AWS CloudFormation, HashiCorp Terraform, Microsoft Visio, Microsoft Threat Modeling Tool and Lucidcharts.

According to GlobalData, spending on cybersecurity in the medical device sector is expected to top $1.2 billion in 2025. It comes as manufacturers seek to comply with regulations issued by authorities like the FDA in the US, the EU in Europe, and the NHS in the UK. With IriusRisk, your threat modeling is simplified and allows multiple teams to see results in real-time.

IriusRisk **integrates** with existing DevSecOps processes

Your teams can **collaborate in real-time**



IriusRisk provides a **central platform** for multiple departments to view, prioritize and fix potential threats

## How it works

IriusRisk's platform automatically analyzes security weaknesses and threats in cloud native designs without drawing an architecture diagram.

It generates a threat model from an IaC descriptor, and as DevOps configure multiple IaCs during the development lifecycle, it's easy to see why our automated process is invaluable. Identifying threats in this early-stage development means you can fix and make safe far cheaper and more easily than if vulnerabilities are found further down the line or (worse) when a device is hacked.

It's why the National Institute of Standards and Technology (NIST) in the US recommends automated threat modeling.

## Why IriusRisk

Nailing down your security does not have to be slow or expensive. Partner with IriusRisk for an easy-to-use and automated threat modeling platform that identifies security flaws in architecture before you build.

We're recognized as a leader in threat modeling, trusted by the public sector, tech, and financial services companies worldwide. We bring our years of experience and success to the medical device sector, making your teams more agile and successful across the many applications they develop and maintain.

And most importantly, your company won't risk the cost and reputational damage caused by a cybersecurity attack.

Don't just take our word for it. Book a consultation with our threat modeling specialists to see the extraordinary benefits IriusRisk will deliver to your development teams.

Book now