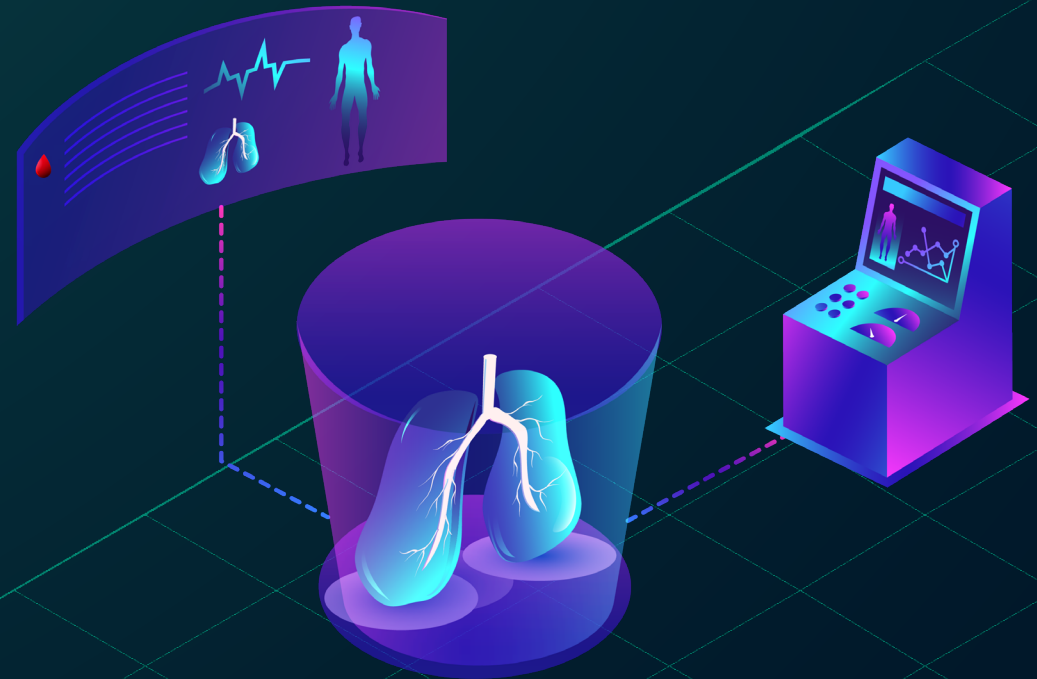


## CASE STUDY

**A medical device company uses IriusRisk Threat Modeling to make medical devices safer and more secure for its patients and users.**

**IriusRisk**

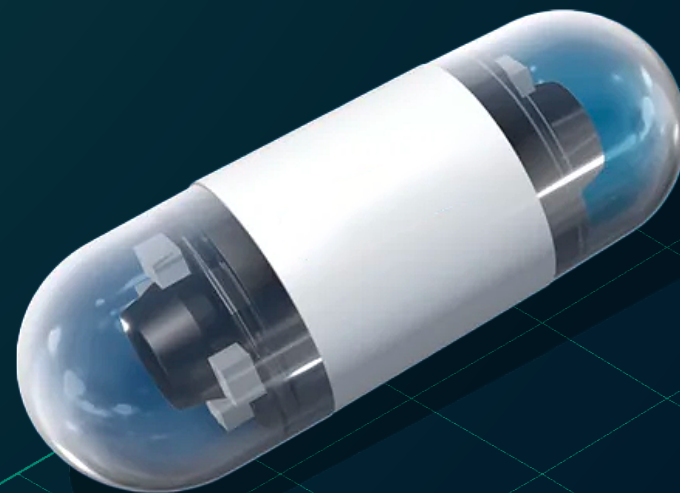


# The company automates risk identification and mitigation

A medical device company operating globally, implements robust security practices and regulation activities, to achieve its mission of extending the life, and quality of life, of its patients.'

Part of the process for a new device is to obtain FDA approval. In this case it was necessary for the Next Generation of an internal medical device software and hardware, to ensure the product is secure and ready for market. They were operating using one single very large Visio diagram, which successfully mapped out their architecture, however identifying risks was a manual and time-consuming process. And there was no single source of truth for this diagram and subsequently the product.

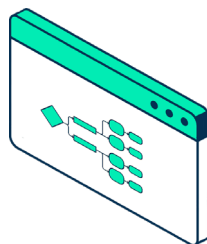
Due to being a medical device manufacturer, the company, has to ensure compliance to several standards and regulations set out by the FDA. Using an isolated diagram without any risk or mitigation output, was not going to support the efforts of the Security Team. This small and busy team would likely need a partner to support them using an Automated Threat Modeling Tool such as IriusRisk.



# Testing, remediation and FDA approval



Using the On-Premise version of IriusRisk, and storing data locally, the company, decided to threat model the internal device as its first medical device. With a very complex diagram and multiple connection points, coupled with a small resource to work on this, the company needed to lean on IriusRisk and its partner network for support.



In addition to this, a lot of documentation is to be provided in order for the FDA submission to be completed, and therefore the company required a tool that would support in identifying and prioritizing risks, suggesting mitigations, while also understanding compliance requirements and allowing the Security Team to rely on it for regulatory assessments.

“As part of the submission and the medical device development and designing, we needed a lot of risk assessments. This is a big part of it especially when the software is in the cloud connected to networks, the internet and other systems. So we needed a very deep security risk analysis.

**Product Security Engineer**

The company, also has a small Security Team for this particular division. So resources were low to be able to scale out a solution at speed. A partner would be needed in order for the team to get value more effectively.

## Security Team independently creating threat models and managing risks in an automated and repeatable way.

Accenture supported the company, to build their first diagram in IriusRisk. From here, the collaborating teams at Accenture and the company were able to use components that came as standard, while also having the flexibility to customize the Security Libraries to fit the requirements.

“ There were big advantages to using IriusRisk. After building our diagrams and processes for the cloud we used a lot of predefined components within IriusRisk. We got lots of applicable threats and also the controls for mitigating the risk. We were used to threat modeling manually and debating the mitigations between the security engineers. So the big advantage is having the prioritized threats, the weaknesses and the suggested controls of that threat as part of the tool.

Product Security Engineer

Thanks to bespoke training sessions from Accenture, the Security Team is now able to continue threat modeling independently, with a training program planned to roll this out more broadly and across other departments. This timing coincides with the next project for this Business Unit, which is about to start, and will go through these defined threat modeling processes.

# Benefits of using IriusRisk:



## Customization:

The company was able to add its own unique hardware components, and custom rules to further improve the results of their threat model and associated risks.



## Time saving:

Automating threat modeling processes with IriusRisk has saved crucial time for a small team working on the threat model project and its required actions.



## Training Certification:

The IriusRisk Training Certification is supporting this business unit to roll out the tool to other teams and gain broader buy-in.



## Partner collaboration:

IriusRisk's Partner Network was a great support to build the very first complex threat model and include all of the right content for the project.



## Prioritized risks and controls:

Being able to automate this output to see a list of risks and countermeasures has been a benefit in terms of time and resource.



## Supports compliance:

IriusRisk allowed processes and documentation to be provided to the FDA to obtain approval on the first device in this project that was threat modeled.

How would you sum up the benefits of IriusRisk in just one sentence?

**“ There have been lots of advantages, but the main thing is that there’s one place and one structure to automate the first stage of our threat analysis.”**

Product Security Engineer