CYE

Hyver Saves a **Medical Device Company** from Five Years of Disruption

The Problem:

Vulnerability in New Product Threatens FDA Approval

A medical devices company was weeks away from launching a digital product that was projected to be used by 500,000 people in the US.

Since the client operated in one of the most highly regulated industries, many of its medical products had to receive a green light by the FDA before going to market. Before launch, the client's security team asked CYE to make sure its security met the highest standards.

Hyver conducted a baseline assessment of the product's security posture, covering external attack surfaces and cloud environments from a variety of threat sources including internal, external, and third party. Analyzing the findings across the client's attack routes, Hyver quantified the risk exposure according to likelihood and business impact.

Critical Finding: World's Most Costly Data, for Free

Hyver found a critical vulnerability in the product's core. Through an unprotected API, any user was able to retrieve health records (PHI) through simple manipulation of the user's Social Security number. If this had been discovered and used by malicious actors, the client's reputational damage, as well as financial penalties, would have been substantial.

$210,000,000 Risk Exposure

{ **$420** Cost of PHI Breach
X
500,000 Future Users }

Root Cause: Internal Product Turning Public

The problem started because the device's original purpose was to serve only the medical staff. Due to the restricted access, the client had decided to lower protection on other interfaces such as API. Pivoting the product purpose without code redesign had made it relatively easy for hackers to obtain sensitive information.

The Solution:

Addition of Security Layer to Avoid Reapplying for FDA Approval

The product had a critical issue that had to be fixed through infrastructure adjustments. The textbook solution would have been changing the source code. But since this meant restarting a five-year submission process to the FDA, it was not a valid option. Instead, Hyver identified a significantly more cost-effective plan.

> **"This is another unfortunate example of why compliance does not equal security."**
>
> Reuven Aronashvili, CEO of CYE

Hyver's graph analysis found an alternative. It concluded that adding another layer of security could solve this problem without having to reapply for FDA approval. It also found that coupling the session with the SSN enabled only one device to view the health records that were related to the specific session. Later, this solution was streamlined to avoid double sign-ins.

The Impact:

Better Product Security and Enhanced Cybersecurity Maturity

CYE helped the client block the users' ability to change API queries after they had been sent. In addition, patients were notified every time their data was accessed.

Today the client is well on its way to reaching its business goals and uses Hyver to continuously take proactive steps to enhance its security maturity.

> **"I've worked with numerous vendors over the years and I don't believe any of them could have solved this problem like CYE did. Their business mindset is a game changer for the industry."**
>
> VP of Information Security, the Client

About CYE

CYE's optimized cyber risk quantification platform and expert guidance transform the way organizations manage cybersecurity. Using AI, machine learning, and innovative technology, CYE visualizes attack routes, quantifies, mitigates, and communicates cyber risk, and matures organizational cybersecurity posture. In doing so, CYE provides clear and relevant insights that empower companies to make effective cybersecurity decisions. The company serves organizations in multiple industries globally. Founded in 2012, with headquarters in Israel and operations around the world, CYE is funded by EQT Private Equity and 83North. Visit us at cyesec.com.

CYE