ZIMPERIUM

How a major global health tech firm built security into IoMT apps to protect IP and patients

Industry
Health and Pharma Technology

Location
International Scope

Solution
zKeyBox
zShield

Customer Profile

This major health technology and pharmaceutical manufacturer delivers cutting-edge monitoring, dispensing and diagnostics technologies, and drugs used by healthcare providers and their patients worldwide. The company owns several leading healthcare brands and has been at the forefront of medical innovation for decades.

The Challenge

The recent growth in wearable health monitoring and drug delivery systems brings enormous improvement in the quality of life to many chronic disease sufferers, enabling easier and safer monitoring of conditions, as well as automatically adjusted intravenous drug delivery. Yet Internet of Medical Things (IoMT) companies, such as the one profiled here, face multiple challenges.

The company's solutions deal with sensitive personal and medical data that must be protected at all times. Both from a responsibility and a regulatory standpoint, the company is expected to ensure data is stored, managed, and transmitted securely. The solutions also include valuable proprietary algorithms and technology that require safeguarding.

To maintain its competitive advantage, in addition to the critical task of securing patient data, the company needed to protect its intellectual property from theft, re-use, and to prevent tampering with its device application code.

As a supplier in the medical market, it also needed to ensure compliance with various regulations and policies, including:

- USA: UL 2900-1, HIPAA, US Postmarket Management of Cybersecurity in Medical Devices
- Europe: GDPR, the EU Medical Devices Regulation, the In-vitro Diagnostic Medical Devices Regulation
- International: ISO/IEC 27001 Information Security

For savvy medical device companies, regulatory compliance is more than just observing best practices concerning healthcare security and ensuring access to markets; it is essential for mitigating cyberattacks when they do happen and minimizing the financial impact of any breaches. The high value of the data at stake means that healthcare companies are constantly under attack. Stolen healthcare data is worth three times as much as other types of PII[1] and the healthcare sector has the highest breach costs of any industry globally, with an average total cost of $6.45 million.[2]

Challenge Highlights

- Meet strict compliance rules ensuring personal data is kept secure Deliver cryptographic protection for encryption keys
- Protect proprietary algorithms from being extracted and copied or tampered with
- Common platform required for desktop, Android and iOS applications
- Deploy a solution with minimal impact to the software development process

The Solution

The company provides wearable technologies that continually take readings from the users and upon request, transmit this data to a mobile device. The technology also exposes an API that can be used to connect to third-party drug delivery systems. Both the application and the data communicated through the API need to be secured.

The company investigated an array of low-cost and free obfuscators available in the market, but found they provided inadequate protection for their needs. It also evaluated full-featured commercial application shielding solutions, determining that many were difficult to use and would over-burden existing development processes.

The team needed a single solution that worked across multiple platforms, including desktops and mobile devices, yet was simple to integrate and had minimal impact on their software development lifecycle. In the end, the company chose Zimperium to keep its proprietary algorithms and customer data safe.

Zimperium's zShield shields IoMT applications

The company chose the Zimperium suite of products to protect their keys from extraction and the integrity of their code. The Zimperium solutions support all major operating systems and are purpose-built for ease of use along with enterprise-grade protection.

With the assistance of Zimperium expert support, the team quickly got up and running, seamlessly embedding Zimperium's tools into the existing build systems. Once set up, the protection proces s becomes near invisible to developers; a secure application is automatically created at build time. The company leverages the advanced obfuscation, anti-tamper, and runtime application self protection (RASP) capabilities in zShield to stop anyone from reverse engineering its applications, accessing its intellectual property, or modifying the behavior of applications.

Zimperium's zKeyBox keeps cryptographic keys safe

It also employs zKeyBox, a white-box cryptography solution that ensures encryption keys—essential to keep IoMT communications and data secure—remain protected at all times. The company was especially concerned about securing keys during cryptographic operations to prevent them from being exposed in memory and able to be extracted by side channel attacks. A powerful, drop-in replacement for standard cryptographic libraries, zKeyBox is one of the only solutions in the world currently able to protect keys against most types of side channel attacks.

> Our primary goal is protecting our IP and preventing its reuse or exploit by others. Zimperium does an excellent job creating and maintaining security around this product line used by millions of people. This builds trust with our customers, whom we are dedicated to serving.

The Results

By deploying the two Zimperium solutions, the company improved its security posture with additional layers. It has turned its software into autonomous, self-defending applications, thereby keeping patient data, proprietary algorithms, and encryption keys safe.

Free up dev team to focus on innovation

In the four years that the company has been using Zimperium, it has continued to innovate in more connected approaches to improve care. The development team is not hampered or slowed down by cumbersome app security tools.

Secure IP and data

The company has constantly increased interoperability and expanded hardware partnerships, secure in the knowledge that information can be safely exchanged without exposing its IP and data to attacks. The company's IoMT applications remain protected from penetration by static and dynamic analysis, hacking, and piracy.

Ensure regulatory compliance

Zimperium's zKeyBox and zShield have helped the company adhere to the various regulations governing healthcare data, and medical device and application security. For example, UL-2900-1, adopted by the FDA, requires the use of cryptographically secure mechanisms and that mitigations are in place to protect against vulnerability exploits and software weaknesses. The company uses multiple features available in zShield to prevent static analysis and shield its applications from real-time attacks, including detecting any tampering or inspection attempts and automatically triggering a custom defense function. zKeyBox strengthens the cryptographic mechanisms used by the device app, ensuring that encryption keys are always encoded.

1. Healthcare Cyber Heists in 2019,VMware Carbon Black, May 2019
2. Cost of a Data Breach Report 2019,Ponemon Institute, July 2019

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 7524