The Medical Device Cybersecurity Challenge

Although connected medical devices undoubtedly provide numerous benefits for healthcare providers and patients alike, they also have one glaring fault - their security levels have not kept up with their rapid proliferation, making them attractive targets for cyberattacks and increasing the security risks for organizations across the healthcare ecosystem.

Unresolved device security issues can lead to results ranging from simple inconvenience to disastrous consequences. When it comes to the healthcare industry, as has been shown over the past few years, attacks that exploit vulnerabilities on connected medical devices can disrupt vital services, cause significant financial losses, and above all, pose a risk to patient safety.

The rapid increase in customer and regulatory demands for device security, alongside the rising levels of reputational, monetary and legal risk due to new vulnerability exposures and offensive activities, has led to device security becoming strategic imperative for medical device manufacturers.

To protect their business and reassure both regulators and customers, medical device companies must integrate security across all their connected products and during the entire device lifecycle, both before and after deployment. This requires the tools to effectively assess, control and manage the risk levels of their connected products, including devices and components sourced from third parties, and to react quickly when new vulnerabilities or threats arise.

The challenge is that implementing these capabilities usually requires multiple disparate point solutions which are hard to manage and integrate, as well as considerable internal resources and security know-how.
About Vdoo

Vdoo was founded by serial entrepreneurs who previously sold cybersecurity company Cyvera to Palo Alto Networks, bringing with them extensive knowledge of endpoint and embedded system security. The company has raised $45 million from top-tier investors including 83North, Dell Technology Capital, WRVI Capital, GGV Capital, NTT DOCOMO and MS&AD ventures. Vdoo has offices in the US, Europe, Japan and Israel, and dozens of well-known global customers.

For additional information, please contact us at info@vdoo.com or visit our website at https://vdoo.com

All Rights Reserved to Vdoo Connected Trust LTD.

The Vdoo Integrated Device Security Platform

The Vdoo Integrated Device Security Platform is the only automated device security platform that covers the entire device lifecycle – from design, development and testing to deployment and maintenance.

Our platform includes everything that medical device companies need to secure their connected products consistently at scale. It provides interconnected capabilities including in-depth device security analysis, easy-to-follow gap resolution guidance, compliance validation, embedded protection for deployed devices, ongoing vulnerability monitoring and actionable device security insights.

The Vdoo Approach to Device Security: Comprehensive, Efficient and Automated

Vdoo’s device-centric platform is designed to simplify the process of implementing security across devices, providing broad security coverage while minimizing time-to-market and functionality impact.

- Performs automated analysis of the device's firmware binary image, detecting a broad range of known security issues and potential zero-day vulnerabilities without requiring source code access
- Provides device-specific impact assessment and clear step-by-step guidance for quick issue resolution
- Protects devices against new threats post-deployment through ongoing monitoring and an automatically tailored embedded device protection agent
- Supports compliance efforts by mapping discovered security issues to industry regulations and standards as well as providing needed security controls to achieve compliance

Why Use the Vdoo Integrated Device Security Platform?

Lower security risks
Quickly detect and resolve threats at every stage of the device lifecycle

Increase efficiency
Focus on the highest priority issues and enable fast resolution without the need for internal security expertise

Gain visibility
Control supply chain security with full visibility into third-party products without access to their source code

Simplify security integration
Integrate device security capabilities into existing development, operational and asset management systems

Shorten time-to-market
Perform on-demand automated security analysis in minutes rather than manual processes that take months

Speed up compliance
Quickly validate compliance with requirements in UL 2900-2-1, FDA medical device cybersecurity guidance and more