VDC|Research
Insights for the Connected World

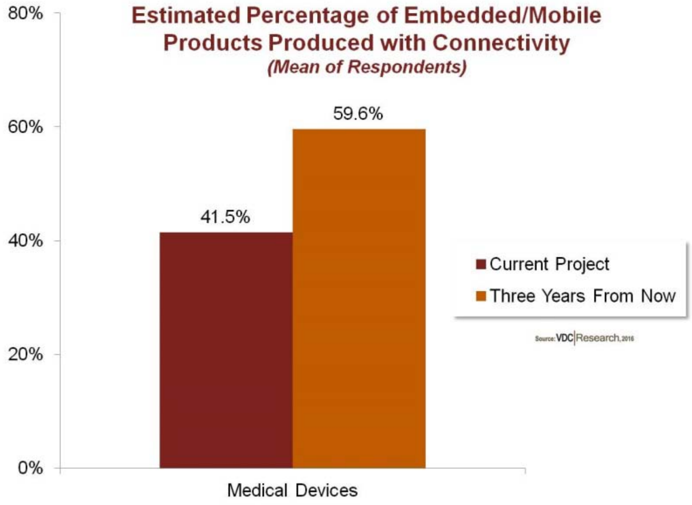
Press Release

Connected Medical Devices Are Sick with Vulnerabilities, According to VDC Research

Medical devices manufacturers are struggling to safeguard their newly connected designs from current and emerging security threats.

“No industry lags embedded security requirements for connected systems as much as the medical device sector.”

Natick, MA (PRWEB) January 29, 2016



Source: VDC|Research, 2016

The medical device sector will be among the fastest growing markets for embedded security software through the next five years, according to a new report by VDC Research (click here to learn more). The market for medical devices spans a variety of hardware profiles including high-performance imaging systems, mobile diagnostic equipment and pumps, and wearable or implantable devices. Until recently, the majority of medical device manufacturers and others within the ecosystem treated security as an optional value-add under the misconception that their devices/products did not produce valuable data or would be a target for a hacker. The Internet of Things has enlarged the crosshairs on medical devices as such systems become more accessible and integrated with enterprise hospital platforms.

“Connectivity can enable a slew of valuable medical device and health care applications, but at the same time potentially expose manufacturers and end users to new security vulnerabilities,” says VDC analyst Daniel Mandell. From VDC Research’s 2015 IoT & Embedded Engineering survey, respondents from the medical device sector indicated that three years from now nearly 60% of embedded/mobile systems produced by their organization will feature connectivity – up from 41.5% currently. “Historically, medical systems have been isolated or air-gapped from health care networks, so device manufacturers today are contending with implementing years-worth of security advancements that are already commonplace in other embedded verticals,” says Mandell. “A single networked device has the potential to compromise an entire hospital network.”

Rectifying the security issues facing medical devices and health care networks will require dramatic changes to embedded development and technology adoption, prioritization of resources (both for embedded device hardware/software and hospital IT infrastructure investments), and end user training. Most medical device manufacturers do not have the capability to stay at pace with the evolving threat landscape while still contending with growing regulatory and standard requirements – never mind differentiating products and solutions themselves within a highly competitive market. The door is open for security solutions providers to come to the aid of fledging OEMs… as well as for hackers for exploitation.

About VDC Research

Founded in 1971, VDC Research provides in-depth insights to technology vendors, end users, and investors across the globe. As a market research and consulting firm, VDC’s coverage of AutoID, enterprise mobility, industrial automation, and IoT and embedded technologies is among the most advanced in the industry, helping our clients make critical decisions with confidence. Offering syndicated reports and custom consultation, our methodologies consistently provide accurate forecasts and unmatched thought leadership for deeply technical markets. Located in Natick, Massachusetts, VDC prides itself on its close personal relationships with clients, delivering an attention to detail and a unique perspective that is second to none.