dispersive technologies™

Secure Your Remote Patient Monitoring With Dispersive™ Virtualized Networks

Nearly five million patients around the world were remotely monitored in 2015—a staggering 51% increase from the previous year. According to Swedish research firm Berg Insight, that number will grow to 36 million by 2020.[1]

The remote patient monitoring (RPM) juggernaut will continue to attract physicians, healthcare facilities, investors and startup tech companies. However, there's another segment with a keen interest in these devices: cybercriminals.

Hackers pose a very real security threat to your RPM devices, one that demands a very real security solution.

Dispersive™ Virtualized Networks.

Realize It's A Life-And-Death Issue

Breaches of RPM systems can do more than compromise data or expose a health crisis of an enemy or competitor. They literally can take lives. Hackers can override an insulin pump's radio control, disable its vibrating safety alert, and dump a lethal dosage into the unwitting patient. Using just a laptop computer, an attacker can kill a pacemaker wearer 50 feet away by commanding the device to emit an 830-volt shock.

(Concerned about such an assassination attempt, Vice President Dick Cheney directed doctors in 2007 to disable his pacemaker's wireless capability.)[2]

Both the DHS and FDA have issued warnings to hospitals and health providers, urging them to address the cybersecurity threats posed by Internet connectivity and mobile devices like those used in RPM. Those who do not could be vulnerable to lawsuits or government crackdowns.

Divide And Conquer

Dispersive™ VNs can help you defend against cyberattacks while providing superior speed and reliability to RPM.

These software-based solutions run on any off-the-shelf hardware using any operating system—Microsoft Windows, Mac OS, Linux or Unix. There's no need to purchase new equipment or endure an OS learning curve.

With conventional RPM networks, one device (e.g., a heart monitor) sends one constant stream of data to another device (a monitoring machine) along one networking path. This one-stream, one-path approach creates a single point of failure due to congestion. It also provides a huge stationary target for hackers.

Dispersive™ VNs take a more intelligent approach. The software employs a divide-and-conquer strategy. It parses the monitoring data into smaller, independent packet streams and sends them randomly down available paths. These packet streams are then reassembled at the receiving end. If one of the paths becomes congested, the software instantaneously

1 "4 Key Statistics On Remote Patient Monitoring Growth," Akanksha Jayanthi, *Beckers Hospital Review*, December 8, 2015. **2** "Doctors Disabled Wireless In Dick Cheney's Pacemaker To Thwart Hacking," Lisa Vaas, *Naked Security by Sophos*, October 22, 2013.

rolls the data in that channel to a trouble-free route. If one of the packets is lost in transmission, the software automatically requests a resend.

Dispersive™ VN software continuously monitors the health and performance of each independent pathway. When problems are sensed on one path, it automatically and instantaneously rolls traffic to new paths. As a result, your data bypasses bottlenecks and avoids router failures.

Thanks to this multipath approach, Dispersive™ Virtualized Networks send data up to ten times faster than current virtual private networks (VPNs). And they are more reliable.

Thwart Man-In-The-Middle Attackers

However, the most important advantage of Dispersive™ VNs is tighter security. They present a mind-numbing challenge to even the most ambitious man-in-the-middle attackers.

First, data is not transmitted in one stream. It's divided into individual packet streams and then sent along multiple independent paths which are constantly changing. Message encryption varies from path to path during the session. It's virtually impossible for man-in-the-middle attackers to know which routes you are using, much less collect enough meaningful data to reassemble your communications.

Dispersive™ VNs also feature a built-in firewall that virtually air gaps devices, data and users. This provides a superior way to segment collected patient information from other devices on the network.

As of this writing, there have been no deaths attributed to RPM hacks. However, the possibility exists. And you don't want to be the test case.

Learn more how Dispersive Technologies can bring speed, security and reliability to your remote patient monitoring. Call 1-844-403-5850 or email us at info@dispersivegroup.com.

Find out more: www.dispersivegroup.com

Dispersive Technologies, Inc. | 2555 Westside Parkway, Suite 500 | Alpharetta, GA 30004
Offices in: Dallas | Denver | New York City | San Francisco | Washington, D.C.
Main: 1-844-403-5850 | Sales: 1-844-403-5852 | info@dispersivegroup.com

dispersive
VN by dispersive technologies