EINPRESSWIRE

HOPZERO Protects Network-Connected Medical Devices from Cyber Attack

Unique Security Technology Puts Medical Monitors, Diagnostic Equipment and Patient Data "on a Leash," Governing from What Distance they can be Accessed

HOPZERO

sensitive data belongs on a leash

HOPZERO Protects Medical Systems and Data

AUSTIN, TX, UNITED STATES, May 22, 2019 /EINPresswire.com/ -- HOPZERO Corporation, creator of HopSphere Radius Security, announced its unique flagship product, HopSphere Radius Security, can now protect all manner of network-connected medical IoT devices, biomedical devices including monitors and diagnostic equipment as well as patient records systems. This new approach to cyber security protects critical assets by utilizing an inherent networking principle that puts limits on how far data can travel or from what distance resources can be accessed. As data compromise is on the rise HOPZERO announces a powerful and timely technological breakthrough using network protocols to limit access to medical data and patient monitoring systems.

> Now HOPZERO provides the way to finally eliminate access for attackers and secure inherently insecure medical devices by fundamentally preventing access from outside a medical facility"
>
> *Bill Alderson, CTO*

The resulting breakthrough in network security can establish a "leash" on medical devices and prevent threat actors from gaining access to these devices to:

- Maliciously manipulate them
- Render them inoperable
- Use them as a point to carry out other attacks
- Steal PHI patient data

Cyber security for medical facilities has largely consisted of efforts to protect the network perimeter and use multiple layers of security and access control for computers. While some medical devices have varying levels of protection, most have been found to have vulnerabilities that can be used by skilled attackers.

HOPZERO takes a completely different approach by securing critical medical devices through use of a networking attribute called hop count. Hop count decrements with each router through which data passes.

Every computer in the world has default global hop settings allowing unlimited worldwide data travel distance, HOPZERO sets the limit for each device to only accommodate authorized access. In this way, device communication can be limited to use from within a hospital or medical facility, or even to a portion of the hospital, such as the ICU or to limit communications to only inside the datacenter.

“Network-connected medical devices play a pivotal role in patient health but can also become weaponized through the malicious actions of a cyberterrorist and turned against a patient. The hard truth is that motivated attackers can penetrate any medical facility and commandeer diagnostic equipment, monitoring systems and other medical devices,” said HOPZERO founder and CEO, Bill Alderson.

“Seeing hospital patient monitors open to communicate around the world scares me, firewalls are breached daily because data travel policies are not managed to a lower value. Now HOPZERO provides the way to finally eliminate access for attackers and secure inherently insecure medical devices by fundamentally preventing access from outside a medical facility.”

Cyber threats on medical equipment are growing:

- Over the past year, the FDA has proposed delineating medical devices based on whether they can directly harm patients if hacked [link: https://www.mobihealthnews.com/content/fda-unveils-cybersecurity-attack-response-playbook-medical-devices]

- Recently, Moody’s, the premier source for credit ratings, issued a report warning that the medical device industry is highly vulnerable to cyber risks, largely thanks to the proliferation of insulin pumps, cardiac monitors and other devices that connect to the internet [link: https://healthitsecurity.com/news/hospitals-banks-face-greatest-financial-impact-from-cyberattacks]

- Research from Ben-Gurion University of the Negev shows that skilled threat actors can manipulate 3D medical scans to remove existing medical conditions, or add false ones [link: https://www.medtechdive.com/news/hackers-manipulate-lung-cancer-scans-fool-radiologists-and-ai-software-in/551976/]

- There is now an average of 10-15 connected medical devices per hospital bed in U.S. facilities [link: https://www.alpinesecurity.com/blog/most-dangerous-hacked-medical-devices]

Threats are mounting against HIPAA databases and there is growing demand for regulators and device manufacturers to address the threat of cyberattacks. At the same time, variations on the traditional approaches to security have proven extremely limited. HOPZERO offers a revolutionary approach that is not based on existing security methodology.

Bill Alderson
SecurityInstitute.com
+1 5129659656
bill.alderson@hopzero.com
Visit us on social media:
Facebook
Twitter
LinkedIn