NCHA Strategic Partners
Access. Solutions. Value.

Secure Your Medical Devices and Protect Your Patients

HIPAA, NIST 800-53, and other cybersecurity guidelines focus on securing data; we believe medical device cybersecurity strategies should protect the patient first. CloudWave's SensatoMD (medical device cybersecurity) platform is built on the holistic approach of putting the patients first.

Many medical device cybersecurity solutions only focus on deploying software, and software alone is not a holistic and effective medical device cybersecurity solution. CloudWave's SensatoMD brings together a cybersecurity software platform, 24x7 medical device cybersecurity monitoring and response, policy and procedural templates, end-user awareness training, and medical device incident response. Giving you the holistic protection of all the connected devices by securing patients and data!

"Working with CloudWave is more like working as part of a team versus a typical vendor/client relationship. We previously had no visibility into what was going on with our medical devices because we had no way to monitor them. Having the SensatoMD team monitor all devices on our network is like the golden egg!"

– Patrick Neece, CIO
Lake Regional Health System

SensatoMD

"They pulled us in with their ability to monitor medical devices. They built their environment around tracking medical devices and ensuring that they are secure. No other vendors proposed that ability or focused on it, and making sure medical devices are being kept safe is a big concern in healthcare...

– Klas Survey Response

KLAS RESEARCH

gocloudwave.com

CloudWave

One Solution for Complete Medical Device Cybersecurity

How SensatoMD helps you protect patients.

You may hear from medical device manufacturers that you cannot add technology to monitor your medical devices without voiding the warranty. We confirmed with the FDA that there is one technology that can be added to medical devices without voiding the warranty. That technology is a honeypot, which is included in our medical device program.

The best way to protect patients from a cyberattack on medical devices is to train your clinical staff on how to spot a cyber incident, and more importantly train them on the immediate steps to take to ensure patient safety. The SensatoMD program includes clinical incident response training.

Comprehensive Protection

- Monitor medical device traffic 24x7 with Sensato's Cybersecurity Tactical Operations Center (CTOC)
- Detect threats early with deception technology (honeypots) before a hacker can fully deploy their attack
- Implement medical device incident response planning and training

24x7 Monitoring and Response

- Specialized protocols support clinical engineering and rapid response teams
- Advanced alerts and vulnerabilities review
- Coordinated incident response and tactical forensics

Deploy Best Practices

- Meets or exceeds every aspect of FDA Medical Device Cybersecurity Incident Preparedness and Response Playbook
- Deploy pre-built medical device cybersecurity policy and procedure templates, medical device manufacturer risk assessment framework, team and governance models, and more
- Includes end-user awareness training, clinical engineering/Biomed training, clinical rapid response, and incident response training

Rapid Results

- You get the advantage of time, before and during an attack
- Recognize strong ROI with measurable results
- Receive personalized training and deployment
- Achieve immediate cybersecurity insights
- Deploy in weeks, not months

LEARN MORE AT

gocloudwave.com

CloudWave's Sensato Cybersecurity division is an Information Sharing and Analysis Organization (ISAO) in coordination with government agencies like the Department of Homeland Security (DHS) and the Cybersecurity & Infrastructure Security Agency (CISA), and regularly evaluates and provides guidance about national cyber threats. CloudWave's Sensato team provides real-time threat intelligence about medical devices under their Memorandum of Understanding (MOU) with the U.S. Food and Drug Administration (FDA).