

Rural hospital gains cybersecurity visibility, enables immediate visibility and risk reduction

WHAT OUR CLIENT SAYS





“The biggest peace of mind that this solution provides is knowing that our physical inventory matches the electronic inventory. Vigilor provides remediation steps for our clinical devices and offers the actions to take.”

—Hospital Chief Technology Officer

Problem

- 5% visibility to connected devices
- Network Access Controls blocked visibility to connected devices
- Asset inventories were not updated and required manual collection
- Third party service vendors did not cover medical device cybersecurity and unable to hire necessary expertise in rural area
- Device risks were not identified and unknown

Solution

-  Installed network monitoring hub to detect all connected devices and network activity
-  Network Access Controls update resulted in immediate 100% visibility to connected device
-  Gained visibility to all devices, clearly classified, in a single dashboard
-  New online devices automatically updated and added to inventory
-  Inventory risk identified and remediations immediately distributed for available inventory

Value

- ✓ Full connected inventory **visibility for 100% of IT and medical devices**
- ✓ **Networks being monitored** to catch anomalous behavior
- ✓ **Automatically updating connected inventory** reduces manual workload
- ✓ Inventory classification visibility enables **supply chain decision improvements**
- ✓ Delivered **remediations for 100% discovered vulnerabilities**