CASE STUDY

IoTSecure™

Director of IT - Dodge County Hospital

IoTSecure Solution

IoTSecure's solution was instrumental in addressing these challenges:

The solution was deployed rapidly, in less than 1 hour, without network TAP/SPAN ports or agents. In addition the IoTSA easily handled all their locations with one single appliance.

Next, the IoTSecure solution profiled all the devices on the network to give the I.T. director full visibility into what was on the network, identifying devices by device type so she could make decision about what to remove from the network, as well as what stayed and to which VLAN segment it should be assigned.

After that, IoTSecure continuously and safely checked devices for vulnerabilities and automatically monitored devices for anomalous and malicious communications without any tuning required.

This gave her a near real-time view and alerting into devices at risk, as well as information on how to resolve the issues. Finally, the IT director saved weeks' worth of time on not only on the initial device inventory and monitoring set up, but also on the periodic updates that would be needed so she could spend more time delivering IT value to the business.

Company **Overview:**

Dodge County Hospital is a progressive 94-bed healthcare facility dedicated to meeting the challenges of the changing healthcare environment. Dodge County is also committed to providing quality healthcare for the valued citizens of Dodge County, Georgia as well as the surrounding communities.

Dodge County offers a vast array of services that include an Intensive Care Unit with state-of-the-art equipment. The Education department has diabetic training for patients that have been newly diagnosed. The Emergency Room that services Dodge County offers 24-hour, 7 day a week service by in-house physicians.

Additional departments within Dodge County include the GI Laboratory, Clinical Laboratory, Obstetrics and Nursery, Ophthalmology, Pathology, Pediatrics, Pharmacy, Respiratory, Radiology, Sleep Study Center, and Surgery Center.

The Director IT had these:

Visibility:

She wanted to make sure that there was full visibility into exactly what devices were connected to the network and where they were physically located. This was especially important for identifying any shadow I.T. so it could be safely removed from the network. Additionally findings unmanageable devices and medical devices was important so she could know what to secure and to assist in developing action plans to secure them.

Security:

She also needed to know what devices caused security risks in the network as soon as possible. This included continuous vulnerability testing, device monitoring, and segmentation, as well as understanding the path to resolution to mitigate threats.

Time/ Resources:

As with many I.T. teams, time and resources to conduct manual device inventory and managing security rules for device monitoring was very limited, considering all the other critical I.T. tasks that needed to be performed. She needed a way to automate these time-consuming tasks so she could spend time focusing on delivering IT value to the organization.