Healthcare is something of a big deal. It should be taken very seriously.

Why?

Well, we live in our bodies, and like it or not, those bodies encounter issues. The effects of time, gravity and cholesterol can be rough. Bodies tend to succumb to entropy and break down, and they also, unfortunately (on occasion) run afoul of accidents, resulting in scrapes, bruises, breaks and whatnot.

When these things happen, we want to be attended to in an effective, efficient and hopefully comforting manner. We want our care to be reliable and private, and part of that care depends upon technology.

We understand not only the technology in play within healthcare environments, we’re highly mindful of the context in which the technology is used. We get the big picture and we understand the stakes.

Part of mastering the cybersecurity "lay of the land" – in healthcare and otherwise - is knowing an environment’s terrain. If you don’t know what assets you have, where they are and what they do... they’re kinda hard to defend.

Case In Point

One of our medical center clients needed increased visibility into their IoT and medical devices. They wanted to know everything that was connected to the network and which devices are security risks - because at that time they had no insight/understanding. They needed a solution to identify the devices and then monitor and manage them to lower security risk and exposure. The medical center had a few ongoing monitoring technology partners in mind and asked our advice regarding what would fit their security environment best. We served as a trusted advisor, providing them with recommendations on the features and functions they should evaluate and ensured that the solution would integrate well into their environment to achieve their stated goals.