7 TIPS TO BUILD RESILIENCE AGAINST MEDICAL DEVICE ATTACKS

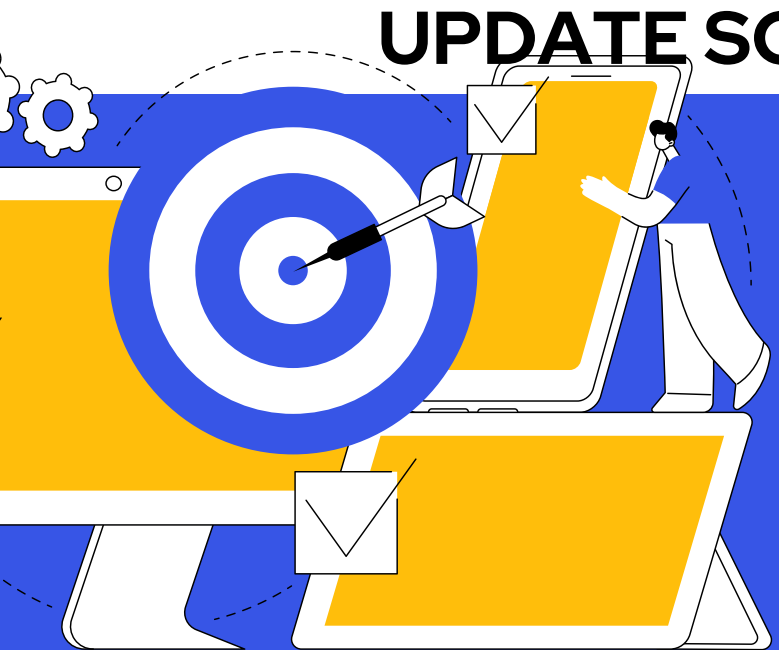
INVENTORY DEVICES

All of it. Your inventory is critical to understanding what is connected to your network.

KNOW THE TEAM

Know who's working with vendors & manufacturers so you can confirm security settings and approved patches.

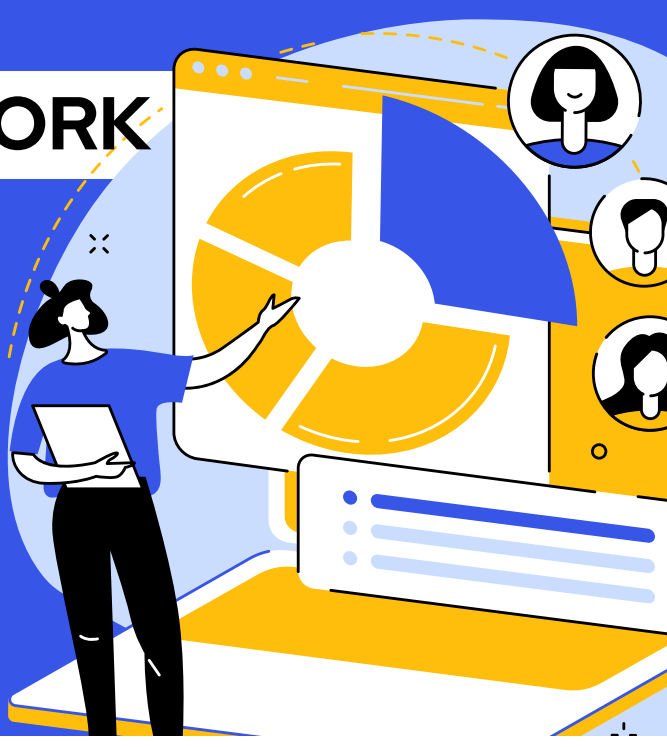
UPDATE SOFTWARE PROMPTLY



Clinical workflows are critical here. They can help your teams understand when and how long a device can go offline.

SEGMENT THE NETWORK

One of the most scalable and effective defenses. Consider which devices talk to each other and the (EMR) and what goes externally.

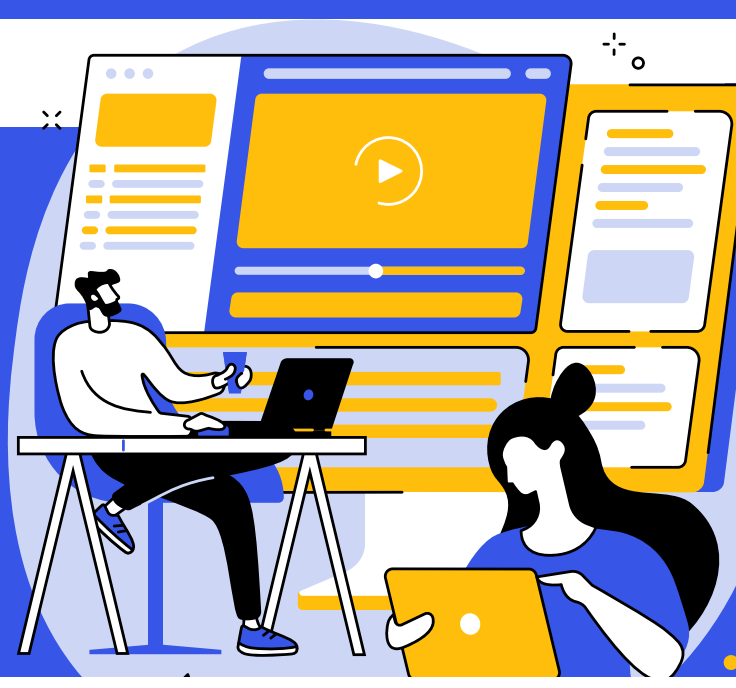


DOCUMENT THE PROCESS

Know what to do when a medical device is compromised. Include steps for responding and recovering from a ransomware attack.

TELL PATIENTS

Make sure patients know how to communicate with you if they suspect a compromise on their medical device.



PRACTICE YOUR PROTOCOLS

Plan making decisions in the moment, like, when to take a device offline, what's safe to use in offline mode or should be taken out of service, how to put the device back into service.

Clearwater