IoT Threat Defense for Medical Systems

Care provided and malware denied

Your hospital is busier than normal with another surge of needs and staff shortages while far away a criminal enterprise has decided that people's pain is to become their profit. The campaign starts like most others, some cursory research followed by a series of phishing emails to overworked billing admins, and their malware arrives.

Fortunately for your patients and staff, clinical systems are separated and protected. You have found classified and segmented systems by function and risk. Only HL7 queries can reach from billing into any care system – file movement is identified, and controlled users of PACS systems are accessed through MFA (Multi-Factor Authentication)-enabled access controls.

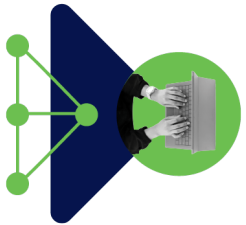
In short Cisco's IoT Threat Defense portfolio of security controls enables healthcare access and malware defeat. People in need receive what is necessary, and people of greed are denied.

Benefits

- Ensure medical system availability
- Medical device identification and visibility
- Mitigation of system vulnerability

Get started with a review of your clinical system architecture today

We can help you find all the connections, intended and otherwise, into and out of your care systems and then apply the right measure of control while assuring continued operation. No system left unseen, and no risk left unaddressed. Ask your Cisco representative or partner for a discussion on where you would like to begin.



Assure clinical availability with inobtrusive controls

Enable improved operations and patient experience with Cisco networking and communications. Assure continued operations with the Cisco® IoT Threat Defense portfolio of integrated protections.

The Cisco solution is comprised of:

- Cisco ISE with AI Endpoint Analytics – draws upon the FDA medical device database to identify and then segment clinical equipment
- Cisco Secure Endpoint – protects both finance and PACS workstations from malware and unwanted applications
- Cisco Secure Firewall – classifies traffic and protects needed applications while stopping exploitation of vulnerable systems
- Cisco Umbrella® – protects and identifies DNS traffic from all your systems, wherever they may be
- Cisco DUO – the easy-to-deploy and easy-to-use multi-factor authentication system for your applications and users
- Cisco Secure Network Analytics – identifies anomalous network traffic as well as applies heuristic-based identifiers for known low and slow abuse patterns.

C45-745068-00 03/22