Q&A with Vivek Sachdev

director of engineering for Invasive Cardiology at GE HealthCare

How GE HealthCare puts IT security in the Cath and EP Labs top of mind

By Gus Iversen

Want to make the IT department feel confident about adding new connected technology to the hospital? Let them oversee every aspect of deployment. That may be the guiding principle behind GE HealthCare's highly-customizable cardiology and electrophysiology recording systems, Mac-Lab™, CardioLab™, and ComboLab.

The skyrocketing rate of cyberattacks on hospitals are well documented, and vulnerabilities can exist in any department. HealthCare Business News spoke to Vivek Sachdev, GE HealthCare's director of engineering for Invasive Cardiology, to learn how simplicity and flexibility can be a potent combination for bringing "defense in depth" security to the Cath and EP Lab.

HCB News: I'd like to dig beneath the surface today and discuss some of the fundamental ways that Mac-Lab, CardioLab, and ComboLab are built for security. Where is the best place to begin?

Vivek Sachdev: Let's start by making sure we understand the technology and what it does. Mac-Lab is a hemodynamic recording system. It's used in the Cath Lab to assist in assessing hemodynamic function of heart. It measures and records patient vitals like invasive and non-invasive blood pressures, heart rate, and ECG signals during a Cardiac Cath procedure to help diagnose and treat coronary artery disease (CAD). CardioLab, on the other hand, is an electrophysiology (EP) recording system used to visualize and record ECG and intracardiac signals. It assists in diagnosis and treatment of cardiac arrythmias (like atrial fibrillation). Then, there's ComboLab, which offers Mac-Lab and CardioLab on the same system and allows for both type of procedures to be performed in the same procedure room.

HCB News: Right. And from a high-level IT perspective, what does it mean to implement these systems?

VS: First and foremost, these systems connect to the hospital's IT backbone, and that's really important to recognize. If something connects there, the IT department needs to make sure it is secure. Other systems in the hospital like scanners, for example, have less connectivity.

Mac-Lab, CardioLab, and ComboLab systems operate on a hospital network. What I mean by that is there is a server, in our case the INW Server, that can be implemented in a virtual environment. And then there are computers, both acquisition and review systems. All of these systems are connected via the INW Server in the hospital IT network to provide desired clinical functionality and workflow.

HCB News: Does that mean Mac-Lab, CardioLab, and ComboLab are supported under the umbrella of a hospital's existing cybersecurity strategy?

VS: That's right and that's one of the complexities. In our case, we give the majority of control to the hospital. In fact, that is one of the benefits of our products. One of the first things we do is provide robust insight into the technology's security through a standard called MDS2, (Manufacturer Disclosure Statement for Medical Device Security). That essentially gives the hospital a full overview of our security posture for the device or software.

There are only a few things we require to be set up in a certain way, which gives the hospital a tremendous amount of flexibility to assess how the technology fits best into their existing infrastructure and cybersecurity strategy. We recommend "defense in depth" through multiple layers of protection.

For instance, the acquisition and review systems for Mac-Lab, CardioLab, and ComboLab come standard and equipped with a secure baseline from Microsoft®. It's something Microsoft makes available for us to use and secures the system better than a general Windows® deployment would. The computer is secure to start with and then the principles of security are applied to the system as its deployed in the network with flexibility around each step of implementation.

HCB News: Can you elaborate on the Microsoft security component?

VS: Access to the system or information is controlled in Microsoft active directory using appropriate policies, groups, and permis-

With Mac-Lab and CardioLab, GE HealthCare is bringing "defense in depth" security to the Cath and EP Lab.

sions. When hospitals configure our systems in their network, they can implement our offered security measures like firewall, anti-virus, user authentication and all patient health information at rest or in motion can be encrypted. The computers for Mac-Lab, CardioLab, and ComboLab use an operating system called Windows 10LTSC. Windows 10 is considered a standard but on our systems LTSC distinguishes our software as a long-term service channel. It's a special edition that foregoes a lot of the added functionalities you'd get on a typical PC in exchange for a core operating system with a longer life cycle. For example, the traditional Windows 10 that is sold now, has an end-of-life of January 2025 from security perspective, but the version of Windows 10 that we currently run has an end-of-life of January 2029 from security perspective. This gives us an opportunity to use a product with a longer serviceable platform and provides a path for security patching over a greater span of time. So, that's a huge benefit for our products.

HCB News: To what extent does the invasive cardiology team need to collaborate with IT on configuration and deployment?

VS: Our project management and field service teams play a huge role and are highly engaged with hospital IT during system configuration and installation. We also provide a comprehensive security guide that speaks to different aspects of security that applies to the product. We have discussed a few of those already. There are a few other key things to think about: how are they keeping systems up to date in terms of security patches? Do they have a business continuity plan? We recommend in our security guide that each hospital have a continuity plan with appropriate backups. For example, if the hospital network is down, can they continue to perform routine or emergency procedures? Yes, our architecture can support an instance where the entire hospital network may be completely down and our systems can still perform a case without any disruption to patient care.

Then there's educating users about security policies. For instance, keeping personal email off the systems. Sometimes those are the easiest way 'bugs' present. So there needs to be policies and procedures in place to train the end user to be cautious and recognize that it's a secure environment.

HCB News: You mentioned patches. How do you keep hospitals up to date on those?

VS: We have a security portal the customer can connect to for a list of qualified

patches. Most who use Windows is already familiar with Patch Tuesday. Every 2nd Tuesday of the month, Microsoft releases security patches. When they release them, we evaluate them right away. Based on the criticality and applicability of the patch, we qualify them in a timely fashion.

machine that can be different. If a nurse or technician needs to take a break during the case and switch to a different user, they can do this within the application.

The benefit here is that IT wants security whereas clinicians want ease of use/workflow – for some hospitals, the default log in is a flexible compromise while making sure that functions performed in the Mac-Lab, CardioLab, and ComboLab applications are appropriately auditable.

> Here we are providing options 'out of the box' but then give the hospital IT department flexibility for anti-virus solutions and security policy deployment based on their preference to be used on the systems.

HCB News: So, if I'm arriving for work in the cath lab, what's my experience like logging in?

VS: We use the standard Microsoft group policy functionality to govern who can and cannot connect to the system. We make sure we can audit who is connected. The default is to have the user who will run the case login and complete the case. This works great if there's only one system operator for a given case. However, we see scenarios where the operator needs to be switched during a case.

HCB News: And that could really disrupt the case workflow?

VS: Exactly. So, the other option that has eased clinical workflow is to have a default log in which allows the system to start up and launch the application, but then present a separate login for a different user to authenticate again within the application. In other words, within Mac-Lab, CardioLab, and ComboLab, the user can authenticate who they are and work within the application. But at a base operating system level, there is one user that is logged into the

HCB News: Earlier you mentioned antivirus, how does that layer fit into the equation?

VS: We think it's valuable to offer flexible antivirus options. In general, there are two types of antivirus software, one is signature based and the other is smart, or heuristic based.

Signature based are what we usually think of first but over time antivirus software has become 'smart' or heuristic in nature. The heuristic antivirus companies – such as Cylance™, Carbon Black™, and CrowdStrike™, to name a few – offer a more AI-based type of protection. We used to only qualify one or two antivirus options and pushed those to our customers, but as we grew along with the IT needs of the hospital, we learned that the customer wants to pick and choose what's most suitable for them.

Today, we qualify about five antivirus solutions, a few signature-based and a few of the heuristic type. Even more appealing is that we have also created a process that allows hospitals to self-qualify any signature-based AV or heuristic AV (in detect mode) that we have not already qualified. With the help of a GE HealthCare Field Service professional, this process provides a path to qualify based on their needs, instead of waiting for us to qualify it for them at a future date.

It's the same as when we deploy the Mac-Lab, CardioLab, and ComboLab systems: Hospitals have certain policies they follow, so we want to give them something basic and let them customize policies how their facility requires. This is another example of that. Here we are providing options 'out of the box' but then give the hospital IT department flexibility for anti-virus solutions and security policy deployment based on their preference to be used on the systems.

HCB News: I am sensing a theme here: customization from the ground up, as a way for hospitals to stay in control of their data and security.

VS: Exactly. The same logic applies throughout Mac-Lab, CardioLab, ComboLab implementations. We provide a path for the hospital IT department to configure their policies and without GE having strict rules. This helps the hospital feel like they've secured the doors and windows of the house exactly how they wanted to. We are making sure the product is securely designed in a way that can be molded to fit their environment. That's the goal.

Share this story: dotmed.com/news/62176