



Lehigh Valley Hospital and Health Network Boosts Network Health with ForeScout CounterACT

“ The ForeScout deployment was easy: it took under a week and is now protecting over 20,000 endpoints. ”

Brian Martin
Information Security Manager
Lehigh Valley Hospital & Health Network

Lehigh Valley Hospital and Health Network (LVHNN) is a premier academic community hospital comprised of three hospital facilities in Allentown and Bethlehem, Pennsylvania plus various Lehigh Valley Health Services (home health, hospice care, and pharmaceutical & health management). In 2007, US News & World Report named Lehigh Valley Hospital one of America's Best Hospitals for the twelfth straight year.

Like many healthcare organizations, LVHNN needed to control levels of network access for authorized personnel such as doctors, nurses and specialists, and visiting guests. Not only did the solution need to distinguish users and devices, it also needed to determine where each user could go on the network once he or she was allowed on. According to Brian Martin, Information Security Manager for LVHNN, “Users were bringing their own and/or infected computers into work, and we didn't want that. Some were computers that weren't compliant with our security policies—they needed OS updates, security patches or anti-virus software installed. Others were hospital property that had been used off-site, picked up malware, and began setting off alarms when they reconnected to the Lehigh network. We wanted a way to control these conditions and let users self-correct the problems.”

Why ForeScout?

Martin and his colleagues had one primary need: the network access solution had to detect and respond to malicious behavior that an IDS wouldn't pick up. After seeing demonstrations from Cisco, ForeScout Technologies and StillSecure, and testing several solutions in their own test network, the organization chose ForeScout for ease of implementation, ease-of-use, and cost effectiveness.

“The ForeScout deployment was easy: it took under a week and is now protecting over 20,000 endpoints,” said Martin. “You hear about NAC being tricky and difficult to deploy, but that hasn't been the case for us. We implemented it in 2007 and the deployment was one of our smoothest.”

How ForeScout Helped

- » Infected mobile devices cannot connect to or infect the network. If an authorized employee brings in an infected laptop and tries to connect, CounterACT will recognize the threat and immediately alert the security team or take direct action to block the laptop from the network.
- » Information Security Manager's job is simplified. *“My job is easier with CounterACT because of its ease-of-management,” said Martin. “CounterACT even determines managed versus unmanaged devices for me, and alerts me when someone comes in with a laptop that's unrecognized. It's automatic.”*
- » Corporate policies are enforced and off-limit applications can be automatically shut down. If an LVHNN employee has an off-limits application on his or her system, the system alerts the security team or can automatically kick it off the network, per the policies set in CounterACT. Martin is especially grateful his team can detect dynamic threats such as hacker activities or new worms, and set up rules to alert or immediately kick the computer off the network.
- » Increased security through visibility and awareness. *“We see alerts on things now that we never saw before,” said Martin. “Before something becomes a problem, we see an alert on intrusions and worms, and we can stop them dead in their tracks. We recently had something trigger a smurf attack and CounterACT let us know it was there before anything went wrong.”*

The ForeScout Difference

Martin appreciates not only the protection against zero-day viruses and worms, but also the network access control capabilities.

“We were looking for a way to ensure the right people could access the wired and wireless networks and only with approved devices. I was bowled over by the detection capabilities of CounterACT,” said Martin.

“That you get a two-in-one intrusion prevention and a NAC solution in CounterACT just makes it that much better. We've known about ForeScout's technology leadership for a while, and have the standalone intrusion prevention ActiveScout appliances deployed, as well. These products just make my life a lot easier: I have less to do to manage them, I can trust that the network's going to stay up and running, and I can see and mitigate malicious activity before it becomes a serious problem.”