

InfoExpress CyberGatekeeper: The Regional Medical Center Customer Case Study

Extending Solid Network Security Practices to the Endpoint

The Regional Medical Center Enables Remote Access in Secure Fashion

Originating from a small private hospital in 1919, The Regional Medical Center (TRMC) has grown into a large acute-care, regional medical center owned by the counties of Orangeburg and Calhoun, South Carolina. It is the result of more than eight decades of work on the part of local physicians, community leaders and citizens to provide top medical care in a wide six-county area. Not only has TRMC focused on delivering advanced medical treatments and programs, but has concentrated on creating a secure and private technology infrastructure to protect the confidentiality of its patients and staff.

Even before the government mandates were delivered in the form of HIPAA regulations, TRMC has practiced the highest levels of computer network security. Strict policies of usage and access have been consistently in place for many years. But, as with many organizations, the requirements for remote and mobile access have grown.

With TRMC, it was apparent that physicians required access to the network from remote locations such as offices and their homes. But the IT network professionals at TRMC knew the vulnerabilities involved with a non- or under-protected remote access. Thus, in 2002, they quickly set out to see how they could enable the productivity gains of remote connectivity but maintain rigorous network security. If they could find a way to enforce the same levels of security policies outside the network as they maintained inside, this would be their ideal solution. Just having users with a VPN connection was not enough, in their estimation.

The search was on for a tool that would work with the corporate issued Cisco VPN on mobile laptop and distributed remote PCs to enforce the configurations and settings. TRMC found the then only game in town - CyberGatekeeper from InfoExpress.

After a brief testing of the CyberGatekeeper Remote appliance, TRMC acquired the InfoExpress solution, and they were extremely glad that they did.

"One of the key factors with going with CyberGatekeeper is that we were not interested in layering more security on top of what we had," says John Garen, a systems analyst with TRMC, "We needed to plug in a solution that would work with our existing infrastructure of firewalls (network and personal), VPN and antivirus."

Two years later, TRMC continues to use CyberGatekeeper successfully as their preferred endpoint auditing and enforcement solution.

"CyberGatekeeper has been fine tuned to run critical checks on each endpoint system as it attempts to enter the network," Garen continued, "It validates that the VPN and personal firewalls are being used, that the antivirus program is installed, running, and patched within a 15-day window."

TRMC uses CyberGatekeeper as a form of intrusion prevention as it looks for pattern files that might be viral or malicious in nature. TRMC is extremely strict about their use of the Internet on the corporate network, and that applies to the users coming in through the VPN. CyberGatekeeper allows TRMC to extend their best practices to outside users, which now include various classes of users, including physicians, administrators and other office and IT staff.

"In addition to the security and the policy enforcement, one of the biggest benefits is there is virtually no maintenance involved with CyberGatekeeper," said Garen. "The appliance continues to run, and we get peace of mind knowing that we are taking valuable steps to protect a patient's sensitive data."

Because CyberGatekeeper has been so successful, there are now plans to expand remote access to other users. Being a major medical facility, there is no way The Regional Medical Center of Orangeburg can afford for their network to be downed by malicious code activities.

CyberGatekeeper is playing a key role to make sure that the network is aware, responsive and protected, at all times.

Customer Requirements

- 1) Compatibility with Cisco VPN and existing client and network infrastructure
- 2) Automatic and persistent network-wide configuration enforcement
- 3) Intelligent scanning or monitoring of all machines that would spot specific pattern files and vulnerabilities

Main Security Issues

- 1) Thwart malicious external code attacks
- 2) Monitor and detect vulnerable, non-compliant systems
- 3) Block admission of potentially harmful devices from network access

Customer Benefits

- 1) Being able to extend tight security policies to remote access users in a consistent manner
- 2) Being able to take advantage of the productivity gains from remote and mobile access
- 3) Improved network and endpoint intelligence and awareness