

# Mercy Medical Center Prescribes Palo Alto Networks for Application Visibility and Control

*“With Palo Alto Networks, we now know what we didn’t know. And it’s scary what some of our users and contractors were doing.”*

—Mark Rein, Senior Director of IT, Mercy Medical Center

## BACKGROUND

Mercy Medical Center is a 130+ year old, Catholic health care facility and teaching hospital for the University of Maryland School of Medicine. Mercy is part of Mercy Health Services, Inc., which also includes Stella Maris, Central Maryland’s largest long-term/geriatric care facility located in Timonium, MD, as well as a network of community health centers. Like any hospital or healthcare organization, the security team must be ever vigilant in protecting the data traversing the network.

## WHEN PARANOIA IS A GOOD THING

In the world of network security, paranoia can be a good thing because it helps the security team stay one step ahead of the next threat. As Senior Director of IT, Mark Rein is paranoid—his job is to implement and maintain a secure network, a daunting task given the open nature of the Mercy Medical Center network and the patient information that needs to be protected.

Like most hospitals, the Mercy Medical Center network has a mix of vendors and contractors requiring access to the network, wireless hot spots for patients, and doctors needing access from all over the campus. Network security is maintained by deploying a layered security architecture complete with locked down desktops to minimize unsanctioned end-user application installations. Even with the existing policies and controls, Mark and his team remain paranoid about unapproved applications and malware.

Always on the lookout for innovative security technology to maintain the upper hand, Mark began evaluating the Palo Alto Networks firewall. The application-centric nature of the Palo Alto Networks firewall showed Mark and his team exactly which applications and threats were traversing the network and that their existing security solutions were unable to see.

As the applications were displayed by the Palo Alto Networks Application Command Center, the team saw non-work related applications such as Skype, Joost, Internet games and a variety of P2P programs traversing the network. In some cases, employees had brought their own computers into the office to take advantage of high speed bandwidth. Intermixed with all this previously unseen traffic were several instances of spyware and adware. Mark put it bluntly, saying “I now know what I didn’t know before and it is a bit scary – these applications represent significant risk to the hospital network”.



### ORGANIZATION:

Mercy Medical Center

### INDUSTRY:

Hospital/Healthcare Provider

### CHALLENGE:

Controlling unapproved application usage, blocking P2P, gaming, spyware and threats.

### SOLUTION:

Palo Alto Networks PA-4020 with policies to control application usage and prevent malware propagation.

### RESULTS:

- Use of P2P, Joost, Skype and Internet gaming has been stopped.
- Increased protection against Spyware, Adware and Trojans.
- Strengthened and enforced appropriate computing resource usage policies for all users.

*“The nimble nature of innovative companies like Palo Alto Networks means I can be a bit less paranoid because we have access to some cutting edge technology which will allow us to keep one step ahead of the ever changing threat landscape.”*

**Mark Rein, Senior Director of IT,  
Mercy Medical Center**

### THE RIGHT PRESCRIPTION FOR UNAPPROVED APPLICATION USAGE

The Mercy Medical Center team saw immediate value in the Palo Alto Networks solution as a means to further protect the network and they quickly moved forward with the deployment of two PA-4020 firewalls in a high availability configuration. Deployed in an active-passive high availability configuration in conjunction with their existing security solutions, the PA-4020s are monitoring all traffic including inbound and outbound Internet traffic, all business partner traffic, as well as all decrypted IPSec and SSL VPN traffic. Policies have been put in place to control unapproved applications and the results have been dramatic, use of P2P, Skype, Joost and game usage on the Mercy Medical Center Network has been stopped. Spyware and adware traffic has been virtually eliminated. Threat prevention has also been improved exemplified by the FTP Trojan Hatu being detected and blocked as it tried to ftp copies of itself every 3 minutes back into the Mercy Medical Center Network.

“Palo Alto Networks has given us a new level of insight into the traffic flowing across our network which we can use to keep our network secure without placing unnecessary restrictions on our users. It is a win-win scenario.” In fact, the increased visibility and control is allowing Mercy Medical Center to re-write their employee policies for appropriate computer resource usage, inclusive of their PC, applications, the network, and Internet access.



**Palo Alto Networks**  
2130 Gold Street, Suite 200  
Alviso, CA 95002-2130  
Main 408.786.0001  
Sales 866.207.0077  
[www.paloaltonetworks.com](http://www.paloaltonetworks.com)