

Encrypting Patient Health Information on Mobile Endpoints

Hospital chooses Trend Micro™ Endpoint Encryption to enable safe, anywhere access to data.

“It is vitally critical for patient privacy, compliance, and our organization's reputation that private data does not get out and that no unauthorized eyes can view it. With Endpoint Encryption, we have full peace of mind that our patient information is secured.”

— Pete Dudenhoefer, Network/PACS Analyst, Millcreek Community Hospital

EXECUTIVE SUMMARY

Customer Name: Millcreek Community Hospital
Industry: Healthcare
Location: Erie, Pennsylvania
Web site: www.millcreekcommunityhospital.org
Number of Employees: 400

CHALLENGE:

- Give physicians, nurses, and technicians access to the data they need at the point of care
- Avoid unauthorized access to sensitive protected health information (PHI)
- In the event of loss/theft, ensure that the data on the hard drive cannot be read
- Ensure compliance with HIPAA and other regulations

SOLUTION:

- Deploy Trend Micro Endpoint Encryption for fully encrypted hard drives and user authentication

BUSINESS RESULTS:

- Improved care, with the deployment of new mobile carts that allow secure, immediate access to crucial patient data
- Full peace of mind, knowing that access to private information is restricted
- Simplicity, with easy set up that takes each device out of service for a minimal amount of time, and reporting that confirms status of all devices
- Instant protection, with data secured while encryption completes in the background

Challenge

Millcreek Community Hospital is a 168-bed hospital specializing in osteopathic acute care. The relatively small organization has garnered a reputation as a regional leader in behavioral healthcare, senior services, and medical education. Today, its physician residency programs number more than any hospital in the tri-state region (New York, Ohio, and Pennsylvania), and are affiliated with one of the nation's largest medical schools.

The technology team has contributed to the hospital's world-class care with solutions that enhance the staff's ability to deliver superior quality care and results. For example, a recent initiative introduced “computers on wheels” or COWs to ensure accurate delivery of bedside medications, provide immediate viewing of results, and give care providers full access to the patient's history and information at the point of care.

Before they could introduce the COWs, the hospital needed a security solution that could meet stringent requirements for data protection compliance. “We started looking at encryption solutions in early 2009, when we were ordering the COWs,” said Pete Dudenhoefer, a network/PACS analyst at Millcreek Community Hospital. “There were three or four solutions we considered. Some were incredibly difficult to use. Some were excellent, in terms of having all the functionality that we needed. We were working with a restricted budget and had to find an easy, affordable solution or the COWs project may have been put on hold.”

Solution

Millcreek Community Hospital found a solution that met all of their requirements: Trend Micro Endpoint Encryption.

Dudenhoefer explained, “Endpoint Encryption has all of the best product aspects—it is simple to install and manage, and gives our users an intuitive interface. Plus it is an affordable solution for an organization of our size with a restricted technology budget.”

The hospital IT department chose a phased deployment, starting with some smaller departments where the functionality was most needed. As the new laptop carts were received and deployed, the hard drives were encrypted and access-restricted with Endpoint Encryption.

“We rolled out Endpoint Encryption in small phases—not hospital wide—because we wanted to minimize the risk of disrupting patient care, and we also wanted to deal with a small number of new users at a time. The deployment process has gone really well, and Endpoint Encryption is very nicely integrated with our Active Directory structure. The only way anyone can access data on a COW is to first use their login/password to authenticate themselves on that device.

Since it continually communicates with our server over wireless, Endpoint Encryption has given us the data security we need for the mobile stations.”

The hospital takes advantage of the existing Ethernet connections to plug-in and initialize the Endpoint Encryption clients, and then the software communicates over the hospital's wireless network to confirm authentication and policy information during operation.

Millcreek Community Hospital has chosen to have Endpoint Encryption fully encrypt each hard drive on the mobile stations. If a laptop is stolen, unauthorized users cannot recover the data from the drive and Endpoint Encryption provides the extra protection of being able to send a “kill” command to the device. When it next connects to the Internet, the device is configured to check in with the Endpoint Encryption server at Millcreek Community Hospital, at which point if the kill command has been invoked it will be instructed to wipe clean its hard drive.

“We have about 50 devices and plan to add another 30,” said Dudenhoefer. “Some devices are shared among a few employees; others might be used by 30 to 40 people. Endpoint Encryption helps me set up and keep track of the policy rules for each device and for the various users. It is all visible and easy to monitor, and really simple for controlling groups of devices and users from the policy server side. And we have the granularity we need to flexibly define accessibility for the various groups’ devices. I can also manage our licenses from the central server.

Results

“Our focus is to provide absolute protection for patient health information,” said Dudenhoefer. “It is vitally critical for patient privacy, compliance, and our organization's reputation that private data does not get out and that no unauthorized eyes can view it. With Endpoint Encryption, we have full peace of mind that our patient information is secured. This is especially important if a device is lost or stolen; with this solution in place, we know that the data on our laptops would be extremely difficult to extract.”

Endpoint Encryption has given Millcreek Community Hospital an easy-to-use and easy-to-install solution. Since the encryption of the full hard drive is carried out in the background, installing the software takes the systems out of service for only a very short time.

“Encryption can take 6 to 10 hours to fully complete, but it runs in the background so that the device can still be used,” said Dudenhoefer. “A nice thing about Endpoint Encryption is that it immediately locks unauthorized users out of the data. Once we start the software, the device is protected and we don't have to wait for encryption to complete to turn it over to the user. When the encryption is done, it reports back to the policy server and reporting shows us all of that status information.

“Endpoint Encryption has been an excellent choice for us, and I would even recommend it for a very large organization with many more devices and users. The simplicity makes it a smart choice.”

“Endpoint Encryption has all of the best product aspects—it is fairly simple to install and manage and gives our users an intuitive interface.”

— Pete Dudenhoefer, Network/PACS Analyst, Millcreek Community

DEPLOYMENT ENVIRONMENT

- 1 hospital site
- 50 endpoint devices (including 25 “computers on wheels”)
- Trend Micro Endpoint Encryption

Company Profile

Millcreek Community Hospital is an osteopathic acute care hospital offering comprehensive inpatient and outpatient services and 24-hour emergency care in Erie, Pennsylvania. Osteopathic medicine's roots center on the belief of the body being able to heal itself. This holistic approach to medicine was brought to Erie in the form of a community hospital over 50 years ago through the vision and efforts of six osteopathic physicians. In 1950, the Erie Osteopathic Hospital was opened. The hospital moved to its current site in 1958, and continues to expand its services and capacity even today with a three-story addition, a new fifth floor, and a Health and Wellness Center. Millcreek Community Hospital prides itself in its commitment to provide the best personal care possible for patients.

Trend Micro Security

- **Trend Micro Endpoint Encryption**
<http://us.trendmicro.com/us/products/enterprise/endpoint-encryption/>

Trend Micro Enabling Technology

- **Trend Micro Smart Protection Network**
<http://us.trendmicro.com/us/trendwatch/core-technologies/smart-protection-network/>



© 2012 Trend Micro Incorporated. All rights reserved. All Trend Micro company, product and service names and slogans are trademarks or registered trademarks of Trend Micro Incorporated. Other names and marks are the property of their respective owners.
CS_MILLCREEK_TMEE_FEB2012

www.trendmicro.com