TREND MICRO™ Securing Your Web World

Truman Medical Centers Implements Trend Micro™ Endpoint Encryption

Meeting HIPAA-HITECH encryption compliance for protection of patient health information and sensitive data.

EXECUTIVE SUMMARY

Customer Name: Truman Medical Centers
Industry: Healthcare
Location: Kansas City, Missouri
Web Site: www.trumed.org
Number of Employees: 4,300 (7,500 workforce members)
Number of End-User Devices: 7,500

CHALLENGE:

- Finding a comprehensive data encryption solution that meets all of the Truman Medical Centers' requirements:
  - Supports multiple device types, operating systems, and full disk encryption (FDE) standard
  - Protects removable media (USB devices)
  - Easy to use and administer
  - Offers comprehensive central management, granular reporting, and auditing
  - Meets "safe harbor" encryption standards (HIPAA, HITECH)
  - Does not increase the everyday support requirements of an already over-tasked IT staff
  - Avoids significant data loss for users

SOLUTION:

- Implement centrally managed Trend Micro Endpoint Encryption for full disk, file folder, and removable media encryption to protect laptops, desktops, and removable media devices

BUSINESS RESULTS:

- Consistent corporate standard for encryption
- Compliance with "safe harbor" encryption
- Strong data protection on laptops, desktops, and removable media
- Enterprise-wide data encryption reporting, logging, auditing, and alerting
- Comprehensive data protection without hindering user productivity
- Reduction in IT overhead due to fewer processes and automated management

> *"In my opinion, Trend Micro Endpoint Encryption should be considered an industry standard for data encryption in healthcare. As an IT leader, when you find a tool that works so well, that's a tool you keep in your tool-box indefinitely. Trend Micro has become an essential compliance and data protection safeguard for Truman Medical Centers."*
>
> **— Rob Jones, Chief Technology Officer,** Truman Medical Centers

Challenge

Due to the vast amount of confidential information that pass through Truman Medical Centers (TMC), a top-priority IT initiative targeted the security of all healthcare and patient information. With regulatory mandates, such as the Health Insurance Portability and Accountability Act (HIPAA) and HITECH Act, that entail significant consequences and penalties, TMC had to implement a strong and flexible data protection solution for thousands of endpoints including mobile devices and removable media. This encompassed several challenges:

1. TMC needed to find a data protection solution that provided full-disk encryption (FDE) on multiple device types and operating systems. The solution must be easy to use, provide comprehensive central management, ensure minimal data loss and have granular reporting and auditing capabilities. TMC recognized that confidential data was not restricted to desktop and laptop computers, and therefore needed a solution that protected portable data on USB devices and other forms of removable media.
2. The data protection solution needed to promote the normal flow of business and meet "safe harbor" encryption standards. With increased mobility comes increased risk of a security breach taking place. Therefore, the data protection solution needed to provide the highest level of protection without impeding employee productivity.
3. TMC needed to select a data protection solution that would not increase the everyday support requirements of an already over-tasked IT staff.

TMC's Vice President and Chief Information Officer, Mitzi Cardenas, understood the risks posed by portable devices such as USB thumb drives. "The last thing we need is to have patient data falling into the wrong hands. It is essential to ensure the integrity and security of healthcare and patient records. Even one incident of data leakage would be disastrous," said Cardenas.

Solution

TMC already had a de-centralized encryption solution in place. Rob Jones, Senior Director and Chief Technology Officer, recognized that it would be extremely difficult to implement multiple data encryption point solutions to cover many different operating systems, users, and devices. “Point solutions are expensive to implement, time consuming, hard to administer, and costly to manage and audit,” said Jones. “They leave huge gaps in managing compliance and lack an audit trail verifying that data encryption was implemented on every endpoint and device.” Jones and TMC determined that they must find a comprehensive and easy-to-use data encryption solution to protect confidential data on laptops, desktops, USB flash drives, and CD/DVDs. The solution must ensure the productivity of its healthcare employees and reduce the numerous disparate processes already in place.

Originally, TMC began to deploy a competitor’s solution on laptops, but determined that it was expensive, tedious to implement, difficult to administer, and that ongoing management was costly and ineffective. The lack of strong key and policy management infrastructure made the implementation hard to support and significantly drove up ticket volume to their help desk. TMC was not willing to scale this solution to cover all of their 7,500 users. Instead, they chose to implement the Trend Micro Endpoint Encryption solution. Trend Micro provided TMC with a simple and comprehensive solution that addressed all of their encryption needs from one enterprise-class platform that includes: Trend Micro™ Endpoint Encryption DataArmor™ module for full disk encryption of desktops and laptops; Trend Micro™ Endpoint Encryption FileArmor™ module for local hard drives and removable media encryption; and Trend Micro™ KeyArmor® module, which is a hardware encrypted USB flash drive with embedded anti-virus protection.

Trend Micro Endpoint Encryption permits multiple users on a single machine through its network-aware capability and flexible policy and key management console. Although Trend Micro Endpoint Encryption protects data on different device types, they are centrally managed by one administrative console and management server. By having one central management server, Trend Micro Endpoint Encryption enables key management, policy management and comprehensive auditing and reporting across all of TMC’s devices and platforms. Plus all connectivity is achieved using standard internet connections. Therefore, TMC did not require additional infrastructure to support the deployment and use of the Trend Micro solution, as a single Trend Micro management server scales to thousands of users and devices. Trend Micro stood out from the other solution providers because of the stellar level of individual, hands-on service it offered. “When you are evaluating – and ultimately deploying new technology – it’s important to have a true partner there to support you along the way,” explained Paul Bean, Senior Security Analyst. “Trend Micro’s support technicians were there whenever I had a question. The level of service Trend Micro offered was a major differentiator.” Trend Micro Enterprise Security products and services are powered by the Trend Micro™ Smart Protection Network™ infrastructure that delivers advanced protection from the cloud. Threats are blocked in real-time, before they reach the customers’ networks.

DEPLOYMENT ENVIRONMENT

25 Locations

7,500 End-User Devices

Trend Micro Endpoint Encryption

- PolicyServer™ Central Management
- DataArmor Module
- FileArmor Module

Trend Micro Endpoint Encryption for Removable Media

- PolicyServer Central Management
- FileArmor Module

Trend Micro KeyArmor

- PolicyServer Central Management

Company Profile

Truman Medical Centers (TMC) is a two-hospital, not-for-profit health system located in Kansas City, Missouri. The downtown location, TMC Hospital Hill, is the largest provider of outpatient specialty care in Kansas City and operates the busiest adult emergency department in the city. It is a top Level 1 Trauma Center in the Kansas City metropolitan area. The suburban hospital, TMC Lakewood, provides a range of specialty and outpatient services. TMC has in excess of 4,300 employees and 7,500 users requiring access to confidential data.

TMC has received top clinical quality ratings from University Health System Consortium (UHC) in the areas of patient safety, performance improvement and adult ICU care. TMC has been named a top performer in heart attack and heart failure care by the Missouri Medical Quality Initiative program; one of “America’s Best Hospitals” for asthma treatment by U.S. News and World Report; a “Top 100 Hospital” by Solucient for rating among the highest in improved patient outcomes and financial performance; a “Most Wired Hospital” by Hospitals and Health Networks; and received the designation of National Center of Excellence in Women’s Health by the Department of Health and Human Services.

Results

TMC is confident that all of their confidential data is protected on mobile devices because of the flexibility of Trend Micro Endpoint Encryption. TMC has the enormous benefit of easily demonstrating their full compliance to regulatory mandates via a comprehensive reporting system that validates security through rapid and real-time reporting. "From an information technology standpoint, one of our most crucial directives is to protect the sensitive data we work with on a daily basis, but it's impossible for me and my team to be everywhere, all of the time, monitoring every endpoint," added Bean. "Trend Micro has become my eyes and ears at the point of impact across the organization. Any time someone tries to access data using an unauthorized device, they are automatically denied and I receive a detailed report documenting the incident. The Trend Micro solution also provides me with detailed logs of every device encrypted. This level of protection enables me sleep at night knowing that TMC's confidential data is safe." TMC believes protecting their patient's privacy and data security is the right thing to do.

"In my opinion, Trend Micro Endpoint Encryption should be considered an industry standard for data encryption in healthcare," comments Jones. "As an IT leader, when you find a tool that works so well, that's a tool you keep in your tool-box indefinitely. Trend Micro has become an essential compliance and data protection safeguard for Truman Medical Center." TMC's use of the Trend Micro solutions have spread to TMC's partners, resulting in additional installs.

"When you are evaluating—and ultimately deploying new technology—it's important to have a true partner there to support you along the way. Trend Micro's support technicians were there whenever I had a question. The level of service Trend Micro offered was a major differentiator."

— Paul Bean, Senior Security Analyst, Truman Medical Centers

Trend Micro Security

- **Trend Micro Endpoint Encryption**
  http://www.trendmicro.com/endpoint-encryption
- **Trend Micro™ Enterprise Security**
  http://us.trendmicro.com/us/home/enterprise/
- **Trend Micro™ Premium Support**
  http://us.trendmicro.com/us/products/enterprise/premium-support/index.html

Trend Micro Enabling Technology

- **Trend Micro™ Smart Protection Network™**
  http://www.smartprotectionnetwork.com

www.trendmicro.com