Hospital Consolidates Security for Compliance and Cost Reduction

Trend Micro™ Enterprise Security Suite builds a cost-effective foundation for added layers of protection.

"Trend Micro helped make vendor consolidation possible by offering a comprehensive data protection portfolio."

—Ty Smallwood, Information Services Security Officer, Medical Center of Central Georgia

EXECUTIVE SUMMARY

Customer Name: The Medical Center of Central Georgia

Industry: Healthcare

Location: Macon, Georgia

Web site: www.mccg.org

Number of Employees: 4,600

CHALLENGE:

- Introduce a better overall vision for security, that strengthens protection and compliance with payment card industry (PCI), HIPAA/HITECH, and other healthcare regulations
- Gain visibility into violation of policies for data protection
- Build in robust controls for restricting data loss through USB drives
- Extend protection to virtual servers and virtual desktop infrastructure (VDI)
- Simplify management of security solutions, from a central location

SOLUTION:

- Upgrade to Trend Micro Enterprise Security Suite
- Introduce Trend Micro™ Threat Management Services, for 24x7 network monitoring
- Add Trend Micro™ Data Loss Prevention and Trend Micro™ Deep Security
- Deploy VMware View™, with virtual desktops protected by Trend Micro VDI security, including agentless antivirus protection for thin clients

BUSINESS RESULTS:

- Better visibility for data protection, with more granular monitoring and control of patient health information and other sensitive data
- Integrated data security controls, for reduced cost and complexity
- More automated, reliable security that meets PCI and healthcare compliance requirements
- Extended life for older PC hardware

Challenge

The Medical Center of Central Georgia (MCCG) often requires that the enterprise security team walk a fine line. "My job is to enforce CGHS/MCCG policies that safeguard patient health information without impeding the ability of our staff and physicians to deliver the best possible care," said Ty Smallwood, Information Services Security Officer at MCCG.

Of course, reducing costs and increasing productivity are always paramount in a large healthcare organization like MCCG. And in recent years, the security team was seeing an alarming increase in the time spent on threat remediation. To reduce operating costs relating to security, they asked their local Trend Micro account team to review their existing proprietary security products and discuss enhancing their existing malware system.

An internal security assessment identified several challenges with the current levels of protection built into the MCCG infrastructure. Besides lacking the latest versions of the deployed Trend Micro™ Enterprise Security solutions, they did not have the visibility and controls they needed for ensuring compliance with the latest industry regulations. It was clearly time to step up the levels of security for the hospital so they could meet and exceed some of the new ARRA/HITECH regulations. The security team also needed a plan that would not add significant costs to an institution that has a lot of pride in their fiscal responsibility.

Solution

With Trend Micro solutions already in place, MCCG was able to take advantage of an easy upgrade to Trend Micro Enterprise Security Suite and affordably introduce many new security advancements. Trend Micro Enterprise Security Suite is part of a tightly integrated offering of content security products, services, and solutions powered by the Trend Micro™ Smart Protection Network™ infrastructure. Together they deliver maximum protection from emerging threats while minimizing the cost and complexity of security management.

Boosted Endpoint Protection

The upgrade gives MCCG new features that include enhanced control over USB devices (for enhanced HIPAA compliance), file and web reputation checks, and an intrusion defense firewall plug-in.

"Taking advantage of the latest features released with Enterprise Security Suite dropped our infection rate by 50%," said Smallwood. "The file and web reputation have been huge for us. It was very surprising to learn the quantity of viruses that we had been exposed to before web reputation checks blocked our users from risky sites. The file reputation catches viruses that try to avoid detection using file name changes.

"Our endpoint security was catching the viruses before at the endpoints, but now the volume of viruses that make it onto our systems is much lower because threats are prevented from making it to our hosts."

24x7 Threat Monitoring Service

Since the hospital's network includes many medical devices and systems that are not owned or operated by the IT staff, the Trend Micro team recommended the introduction of Threat Management Services. This additional layer of security introduces a Threat Discovery Appliance for 24x7 monitoring.

"Trend Micro Threat Management Services has already paid for itself," said Smallwood. "In the first 48 hours, this tool detected viruses on some biomedical devices that were vendor provided and maintained. Bottom line, our policies are only as good as our mitigation and verification. Threat Management Services gives us a layer we never had before—now we can see in real time what is going on. We can monitor the network to detect biomedical device infection and take appropriate action to remediate or isolate the device until remediation is available.

"With the reports from Threat Management Services, we can go back to the medical equipment manufacturers, and push them to patch their machines. This greatly improves the quality of care we provide, and it also helps us avoid legal liability issues in the future by maintaining high standards with our partners. We also use the reports to push for adequate resources to address the types of security issues that the solution highlights."

Data Loss Prevention for Compliance

With high priority placed on HIPAA compliance, the new security deployment also includes Trend Micro Data Loss Prevention and Trend Micro Deep Security. To improve compliance, the security team wanted better visibility into violations of data usage policies.

"We were in the position of not knowing what we didn't know—Trend Micro Data Loss Prevention gives us visibility into data usage behaviors that we did not have before, and provides us with the controls to block risky data flows and drive user awareness via pop-up warnings and user justification screens," said Smallwood. "Initially, we will use this increased visibility to work with the user groups to change processes and mitigate risks. Over time, we will ratchet up controls and block risky behaviors.

"Data protection is a key element in our organization's security and compliance strategy. Trend Micro provides a comprehensive solution portfolio that is easy-to-use, cost-effective and provides us with proven technologies for our endpoint and gateway infrastructure. In order to drive down our capital and operational costs, we adopted a 'best of suite' model versus purchasing multiple point solutions. Trend Micro helped make vendor consolidation possible by offering a comprehensive data protection portfolio."

Results

MCCG is a great example of an organization that improved protection and compliance by consolidating on Trend Micro solutions. The upgrade and additional products and services are actually reducing costs—by dramatically lowering remediation costs, blocking threats before they introduce disruptions to life-critical patient care, and proactively identifying and addressing compliance and liability issues before they arise.

"The deployment of the upgraded endpoint security and new layers of data protection and threat mitigation will continue through this year," explained Smallwood. "We see the benefits of the Trend Micro solutions already.

"In the past, if our CIO or Compliance Officer asked about a security incident, we had to use eight tools and run around our site to gather the information to respond. Today, with Trend Micro endpoint security and data loss prevention alone, we can provide them a volume of information from our central location. Trend Micro security allows us to do more to protect our site, and provide more information efficiently to our users and managers. In healthcare parlance we are now able to reach some 'meaningful use' with the reports we run, and better understand our risks and how to mitigate them."

DEPLOYMENT ENVIRONMENT

4,000 PCs

275 virtual servers (31 VMware ESX hosts)

VMware View, with approximately 80 VDI endpoints in pilot phase

Trend Micro Enterprise Security Suite

Trend Micro Data Loss Prevention

Trend Micro Deep Security

Trend Micro Threat Management Services

Customer Profile

The Medical Center of Central Georgia (MCCG), an entity of Central Georgia Health System (CGHS), is a tertiary regional teaching medical center, a designated Level I Trauma Center, a perinatal center, and is one of 42 twice-designated Magnet® hospitals for nursing excellence. MCCG serves a primary and secondary service area of 30 counties and nearly 750,000 persons in central and south Georgia. It has over 4,600 employees and a medical staff of over 590 physicians. MCCG is the second largest hospital in Georgia with a capacity of 637 beds including medical-surgical, obstetric, pediatric, psychiatric, and specialized individual intensive care units for neurology, pediatric, neonatal, surgical trauma, cardiac and cardiac surgery. The Emergency Center, with helipad capability and three urgent care centers, treats over 120,000 visitors per year. MCCG provides a broad range of community-based, outpatient diagnostic, primary care, extensive home health and hospice care, and comprehensive rehabilitation services. MCCG is the primary teaching hospital for Mercer University School of Medicine, providing residency and fellowship programs for over 100 residents and fellows, and is affiliated with multiple universities as a clinical education site.

The consolidation also translates into reduced operating costs. The simplified management saves staff time, and fewer servers are required to support the integrated Trend Micro solutions.

Smallwood comments, "Trend Micro is moving in the right direction, by consolidating products and suites. Each release builds in more, and the big picture is coming together. Trend Micro is bringing together all the right products into consolidated, cost-effective security solutions.

"Our Trend Micro account team does a great job for us—of all the vendors I work with, they are my favorite. Our Trend Micro account manager understands the issues and as a business partner has proven he truly understands business security threats to our organization. Obviously, our job is easier with one agent on a device and one engine on the desktop. We see Trend Micro moving in that direction, to simplify the technology that we need to address the latest threats."

Next Steps: Securing VDI

With Windows XP approaching end of support life, organizations like MCCG must figure out what to do with older PCs that cannot support Vista or Windows 7 operating systems. Virtual desktop infrastructure (VDI) offers an attractive solution, allowing the deployment of a desktop image that runs within the data center instead of on the local endpoint. Another advantage is the increased control over software and ability to manage security within the data center.

MCCG is taking advantage of Trend Micro VDI Security solutions to introduce virtual desktops on existing PCs as well as new thin client VDI systems. For thin clients, Deep Security offers agentless antivirus protection for VMware View deployments; for traditional PCs and endpoints that need more comprehensive security, Enterprise Security Suite includes the Trend Micro™ OfficeScan™ VDI plug-in.

Both Trend Micro VDI Security alternatives are truly virtual-aware, and operate efficiently within VMware and Citrix environments without overwhelming hypervisors or entire server systems even during scans or updates.

"VDI makes it easy to extend the life of our older PCs," said Smallwood. "We can move forward with the VDI architecture with the confidence that Trend Micro VDI Security makes it easy to secure all of our virtual endpoints. Deep Security even ties into vCenter on the back-end, and so every new agentless virtual desktop is automatically protected without anyone having to remember to load security. Trend Micro gives us very flexible options for securing VDI endpoints, and allows us to match the right level of protection to sessions based on the applications' compliance requirements."

> "*Trend Micro gives us very flexible options for securing VDI endpoints, and allows us to match the right level of protection to sessions based on the applications' compliance requirements.*"
>
> —**Ty Smallwood, Information Services Security Officer,**
> Medical Center of Central Georgia

Trend Micro Security

- **Trend Micro Enterprise Security**
  http://us.trendmicro.com/us/home/enterprise/

- **Trend Micro Enterprise Security Suite**
  http://us.trendmicro.com/us/products/enterprise/security-suite/index.html

- **Trend Micro Data Loss Prevention**
  http://us.trendmicro.com/us/products/enterprise/data-loss-prevention/

- **Trend Micro Deep Security**
  http://us.trendmicro.com/us/solutions/enterprise/security-solutions/virtualization/deep-security/index.html

- **Trend Micro Threat Management Services**
  http://us.trendmicro.com/us/solutions/enterprise/security-solutions/threat-management/key-components/

Trend Micro Enabling Technology

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

www.trendmicro.com