The Medical Center of Central Georgia

THE NUMBERS

- 4,000 PCs, 80 virtual desktops (pilot test)
- 13:1 server consolidation ratios
- $2 million OpEx savings

IN BRIEF

Objective
The Medical Center of Central Georgia (MCCG), like many healthcare organizations, faces intense pressure to reduce costs and increase productivity without sacrificing patient care.

Solution
Several years ago, MCCG transitioned to a VMware virtualized server computing model in the datacenter. This year, it pilot tested virtual desktop infrastructure for added flexibility and cost efficiencies. The organization's Trend Micro security solutions were expanded to ensure protection from threats and compliance with PCI DSS, HIPAA, and other industry regulations.

Business Impact
- Datacenter consolidation, with lowered utility costs and staff-hour savings
- Reduced provisioning times for servers (20 minutes instead of 2 1/2 hours) and desktops (20 minutes instead of 1 1/2 hours)
- Better visibility for data protection
- More automated, reliable security that meets compliance requirements
- Extended life for older PC hardware

Hospital Consolidates Datacenter Servers and Security for Compliance, Autofailover and Cost Reduction

"With VMware, we were not only able to consolidate our servers, but we gained built-in redundancy and failover in the event of any server. Along with failover, Trend Micro security has been key for increasing our confidence in the ability to avoid disruptions to patient-critical services."

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

The Medical Center of Central Georgia (MCCG), an entity of Central Georgia Health System, is the second largest hospital in Georgia. MCCG is also a tertiary regional teaching medical center serving the Mercer University School of Medicine, a designated Level I Trauma Center, a perinatal center, and one of 42 twice-designated Magnet hospitals for nursing excellence.

MCCG serves 30 counties and nearly 750,000 people in central and south Georgia. It employs 4,600 people and has a medical staff of more than 590 physicians. MCCG provides a broad range of community-based, outpatient diagnostic, primary care, extensive home health and hospice care, and comprehensive rehabilitation services.

Consolidation Drives Virtualization Initiatives

Reducing costs and increasing productivity are always paramount in a large healthcare organization like MCCG. Several years ago, the hospital recognized the potential cost efficiencies that could be gained by consolidating servers within the datacenter.

"Since our biggest return on investment could be realized with server virtualization, that was where we began," says Ty Smallwood, Information Services Security Officer for MCCG. "Now we have virtualized about 85 percent of our servers, and we operate with just 431 virtual machines on 32 physical VMware ESX® hosts. We have also deployed VMware® Server to support host operating systems, and VMware vSphere™ and VMware vCenter™ to complete our environment.

"With VMware, we were not only able to consolidate our servers, but we gained built-in redundancy and failover in the event of any server failures," Smallwood notes. "Now, if we lose a hardware server, our VMware environment automatically adjusts the workload within the server cluster. Along with failover, Trend Micro security has been key for increasing our confidence in the ability to avoid disruptions to patient-critical services."

Meeting Increasingly Strict Industry Regulations for Security

During the years since introducing virtualized servers at MCCG, the security team was seeing an alarming increase in the time spent on threat remediation. An internal security assessment identified several security challenges with the current levels of protection built into MCCG's virtualized infrastructure. The assessment revealed that in addition to lacking the latest versions of Trend Micro Enterprise Security solutions, MCCG did not have the visibility and controls it needed to ensure compliance with the latest industry regulations. It was clearly time to step up the levels of security for the hospital's infrastructure so that MCCG could meet and exceed some of the new ARRA and HITECH recommendations.

Integrating VMware and Trend Micro solutions

MCCG was able to take advantage of an easy and cost-effective upgrade to Trend Micro Enterprise Security Suite and affordably introduce many new security advancements specifically designed for virtualized and cloud environments. 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.

Boosted Endpoint Protection
The upgrade gives MCCG new features that include stronger 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 percent," Smallwood says. "The file and Web reputation has been huge for us. It was very surprising to learn the quantity of viruses that we had been exposed to before Web reputation checks began blocking our users from risky sites."

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 System. This additional layer of security introduces a Threat Discovery Appliance for 24x7 monitoring.

"Trend Micro Threat Management System has already paid for itself," says Smallwood. "In the first 48 hours, this tool detected viruses on some biomedical devices...Threat Management System gives us a layer we never had before; now we can see in real time what is going on."

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

Expanding Virtualization to Desktops

With Windows XP approaching the end of support life, organizations like MCCG must figure out what to do with older PCs that cannot support the Vista or Windows 7 operating systems. Virtual desktop infrastructure (VDI) based on VMware View™ offers an attractive solution, allowing the deployment of a desktop image that runs within the datacenter instead of on the local endpoint.

MCCG relies on Trend Micro Virtual Desktop Security solutions to protect virtual desktops on existing PCs as well as new thin client VDI systems. For thin clients, Deep Security offers agentless antivirus protection; for traditional PCs and endpoints, Enterprise Security Suite features the Trend Micro OfficeScan VDI plug-in. Both Trend Micro Virtual Desktop Security alternatives are truly virtual-aware and operate efficiently without slowing hypervisors or servers.

"VDI makes it easy to extend the life of our older PCs," says Smallwood. "We can move forward with our VMware VDI architecture with the confidence that Trend Micro makes it easy to secure all of our endpoints. Deep Security even ties into vCenter on the back end. Every new agentless virtual desktop is automatically protected without anyone having to remember to load security."

The Bottom Line: Reduced Operating Expenses

MCCG is a great example of an organization that has reduced its physical infrastructure without compromising services or security. The combination of VMware and Trend Micro solutions has resulted in many types of savings, from consolidating physical servers to dramatically lowering threat remediation costs.

The consolidation also translates into other reductions of operating costs. The simplified management of fewer servers saves staff time, and the Trend Micro solutions integrate very cost effectively within the consolidated, virtualized server environment. Smallwood comments, "VMware and Trend Micro are moving in the right direction, by partnering on compatible products and suites. With the new platforms and security, the big picture is coming together."

IMPLEMENTATION OVERVIEW

VMware Products:
VMware ESX Servers
VMware Server
VMware View
VMware vShield™ Endpoint
VMware vSphere
VMware vCenter

VMware Services
Technical Account Manager

Applications:
Microsoft Exchange
Clinical systems

Future Application Plans:
vApps

Platform:
Dell Servers
Cisco Networking
Pillar, IBM XIV, EMC, Dell Storage

Trend Micro Security:
Enterprise Security Suite
Data Loss Prevention
Deep Security
Threat Management System