

Kettering Medical Center Network

Facilitating a Healthy and Secure Hospital Network With a Comprehensive Symantec Solution

A major Ohio hospital network turned the need for HIPAA compliance into an opportunity to get a complete network security assessment from Symantec Consulting Services. As a result of this assessment, Kettering Medical Center Network implemented a broad suite of Symantec security solutions which has resulted in greatly enhanced security. The solution is also saving \$218,000 annually in staff time for security monitoring and repairs, and has freed IT staff to develop an application that enables medical professionals to sign on to the network more simply wherever their patients are located. This application will save as many as 1,500 staff hours per day, enabling these providers to provide more and higher quality care to patients.

Company Profile

Kettering Medical Center Network (KMCN) includes five hospitals and 51 satellite facilities in the Dayton, Ohio area. KMCN has 6,800 employees and had net operating revenue in excess of \$600 million in 2004.

Industry

Healthcare

Solution

Information Security

The value of prevention

The healthcare industry is making great strides in improving the quality of care, and technology is driving many of those improvements. Kettering Medical Center Network (KMCN), a group of five hospitals and 51 medical facilities in the Dayton, Ohio area, is at the forefront of this trend.

As an example, obstetrician/gynecologists at KMCN can take advantage of a new labor and delivery application. From any desktop or handheld device in the field, they can now remotely review the vital statistics of an expectant mother in the maternity ward. At a glance they can see when the last possible moment is that they should come in to assist with the delivery, allowing them to safely treat more patients in a day.

For Bob Burritt, manager of network and technology services at KMCN, and his team of 33 IT professionals, supporting this type of new application is their direct contribution to better patient care—and a very high priority for the team.

But another challenge takes most of their time: keeping the 5,000 connected devices of KMCN's network up and running, aiding 7,500 staff professionals in their mission of healing. "Nobody understands the value of prevention like a hospital," says Burritt. "We put a premium on spotting and stopping small problems before they become big ones. And for a hospital network, the number one prevention issue is security."

“Symantec’s intrusion detection appliances, Managed Security Services, and DeepSight Alert Services, and DeepSight Threat Management Services save us \$200,000 a year in staff time.”

Bob Burritt

Director of Technology
Kettering Medical
Center Network

Symantec solutions streamline compliance and enable cost savings of over \$300,000, enabling staff to focus on improving quality of care.

“Symantec showed us it not only had the capability to conduct our security assessment, it also gave us the big picture of what our secure environment should look like—and did so more effectively than any other vendor.”

Bob Burritt

Director of Technology
Kettering Medical Center Network

Safeguarding trust

As patients check in at KMCN, they’re entrusting their health to physicians, and their confidential medical information to KMCN’s network. The federal government recognized the importance of protecting medical information by passing the Health Insurance Portability and Accountability Act (HIPAA). HIPAA sets standards for safeguarding the confidentiality, integrity, and availability of medical records.

It’s no longer just a matter of quality healthcare and sound business practice to ensure the KMCN network is secure and resilient. It’s also a matter of law. The organization must be able to show in an audit that it’s following HIPAA security practices and protocols.

Looking at the big security picture

In late 2003, instead of simply renewing its Symantec AntiVirus™ Enterprise Edition licenses, KMCN decided to conduct a complete network security assessment. HIPAA compliance was one driver, but another was the commitment to be proactive in security. “Given the confidential information that any health organization possesses, we could be severely damaged or put out of business by a security breach,” Burritt says. “In addition, if our network is down because of a security incident, or for any other reason, we calculate that our organization would lose a million dollars of revenue a day.”

KMCN issued a request for quotes for an enterprise security assessment, and 23 security vendors responded. “We took five months to cull the field to eight for interviews and then to three for presentations,” Burritt explains. Of the three vendors that presented, KMCN chose Symantec Consulting Services.

“Symantec showed us it not only had the capability to conduct our security assessment,” Burritt recalls, “it also gave us the big picture of what our secure environment should look like—and did so more effectively than any other vendor. And it has the broad suite of products we needed to make that picture real, and all of them enable HIPAA compliance.

“But we wanted to do more than just comply with HIPAA,” Burritt adds. “With the help of Symantec, we wanted to put into place everything we needed to do our job faster and safer using technology.”

The network security assessment began in October 2004 and Symantec Consulting Services made its recommendations in early February 2005. Over the next several months, KMCN chose and deployed a range of Symantec products and services to secure its environment.

Protecting the perimeter

To provide an outer shield for its network, KMCN chose Symantec™ Network Security 7161 intrusion prevention appliances. These provide real-time, proactive protection against known and unknown (zero-day) attacks and worms. The Network Security 7161 offers both copper and fiber communications interfaces.

In tests by the NSS Group, the world’s foremost independent security testing facility, the appliances, as the test results noted, “blocked 100 percent of attack traffic, while passing 100 percent of legitimate traffic” to lead the field of other tested devices, while accommodating one Gbps of traffic volume.

“We wanted best-of-breed intrusion prevention and the NSS tests confirm we got it,” Burritt says. “What’s more, installation and configuration of the devices went seamlessly, and

we have been extremely pleased with their performance.”

Protection inside the network

Inside the network perimeter, Symantec AntiVirus™ Enterprise Edition protects servers and desktops, and Symantec Client Security and Symantec AntiVirus™ for Handhelds protect laptops and mobile devices. KMCN has relied on Symantec AntiVirus since 1997, when the organization switched from Intel LANDesk because of Symantec’s reputation for security.

24x7 eyes on security

KMCN’s intrusion prevention appliances are continuously monitored and managed by Symantec™ Managed Security Services (MSS), operating from the Symantec Security Operations Center in Alexandria, Virginia. This service uses a state-of-the-art technology platform to aggregate and analyze log data from KMCN’s heterogeneous firewalls, intrusion detection systems, and integrated security appliances. The KMCN network team gets an email from Symantec MSS whenever suspicious activity is spotted that should be investigated.

An added layer of protection comes from Symantec DeepSight™ Alert Services and DeepSight™ Threat Management Services, which provide early warning and actionable information about relevant potential attacks, including prioritization of events according to the threat they pose to KMCN’s network. This information comes from throughout Symantec’s Global Intelligence Network—which consists of five Security Operations Centers, 11 Symantec Support Centers, six Symantec Security Response Labs, and more than 20,000 registered sensors in 180 countries. The cumulative intelligence from thousands of events worldwide gives organizations like KMCN an advantage in separating routine traffic from possible threats.

SOLUTION AT A GLANCE

Business Drivers:

- Support quality of care by ensuring information integrity
- Cost-effectively achieve compliance with HIPAA
- Reduce total cost of ownership (TCO) through enhanced staff productivity, operational efficiencies, and lower licensing costs

Technology Challenges:

- Strengthen network defenses proactively against security threats
- Simplify and centralize security administration while lowering TCO
- Expand role of technology in improving care, while cost-effectively achieving HIPAA compliance

Solution:

Comprehensive enterprise network security solution from Symantec

Symantec Products:

- Symantec Enterprise Security Manager™
- Symantec AntiVirus™ Enterprise Edition
- Symantec AntiVirus™ for Handhelds
- Symantec™ Client Security
- Symantec™ Network Security 7161

Symantec Services

- Symantec DeepSight™ Alert Services
- Symantec DeepSight™ Threat Management Services
- Symantec™ Managed Security Services
- Symantec Platinum Support
- Symantec Consulting Services
- Symantec Education Services

Symantec Licensing

- Symantec Value Program

Technology Environment:

- Applications: IDX CareCast, Cerner QuadRIS, Misys Laboratory, Eclipsys Critical Care
- Databases: Microsoft SQL, IBM DB2, Oracle Database
- Server platform: 200 servers (including HP RP5470, HP DL380, HP ML530, HP BL20P, IBM H50, and Tandem S7600) running a variety of operating systems (including Microsoft Windows 2000 and 2003, HP-UX, IBM AIX, and Novell Netware)
- About 5,000 connected devices including 4,200 desktops and laptops and 300 Personal Digital Assistants (PDAs)

“To check our 200 servers for compliance once took about three to four days. Symantec Enterprise Security Manager cut that to half a day, saving us \$18,000 a year in staff time that we can put to more valuable uses.”

George Bohlen

Network Coordinator

Kettering Medical Center Network

“The Symantec Value Licensing program gives us \$140,000 one-time and \$70,000 annual license savings, along with trimming \$4,000 in yearly administrative time on purchasing and licensing issues.”

Bob Burritt

Director of Technology
Kettering Medical Center Network

After implementing MSS, Bob Burritt and members of his team visited the Security Operations Center in Alexandria and met with the team members there who are responsible for monitoring KMCN’s infrastructure. This visit strengthened KMCN’s partnership with Symantec and gave them an even better understanding of Symantec’s sophisticated security monitoring operations.

More effective monitoring saves staff resources

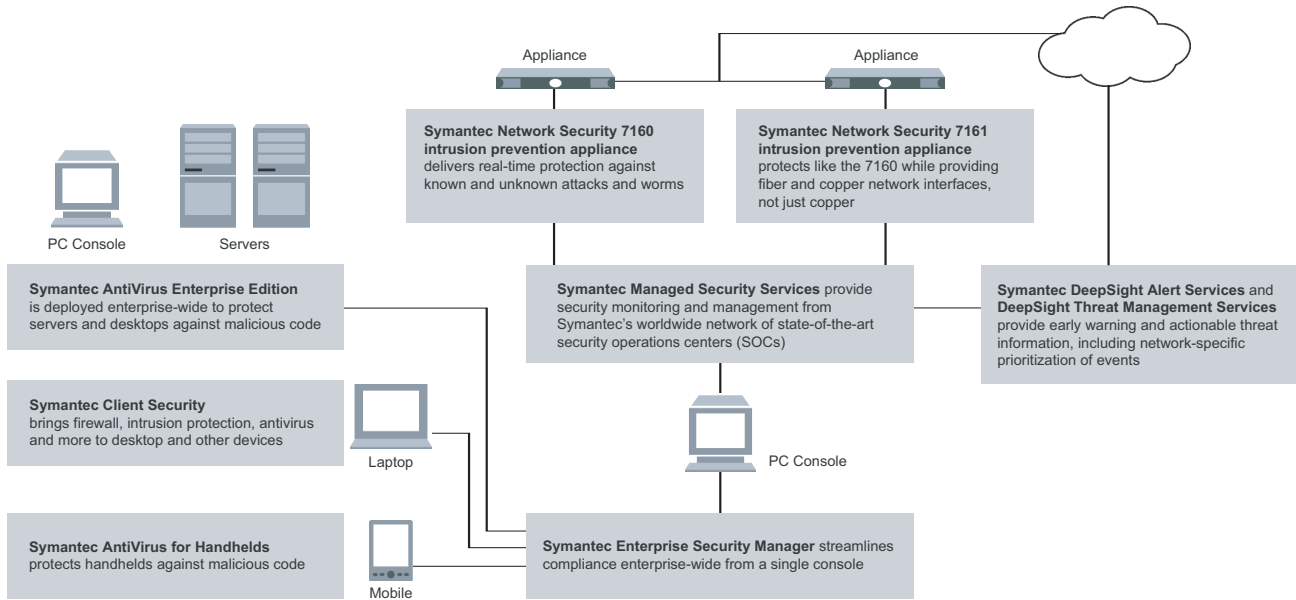
“We tried to provide this level of security on our own,” says Sean Graham, KMCN network engineer. “We had two full-time employees looking at our own IDS sensors at one point. But trying to maintain signatures and updates—while continually inspecting and correlating events from the logs—was becoming quite a feat. Now Symantec MSS is our eye on incidents, and Symantec has a

more informed perspective on threats than we could ever manage ourselves.”

“Just the other day,” Graham recalls, “we were alerted by an email from Symantec MSS to a device in a physician’s office that was performing inappropriate scans, which our Symantec solutions had detected. We immediately shut the port off and had a workstation administrator troubleshoot and repair the system.”

KMCN now needs only occasionally to devote one employee to fix security problems, instead of having two full-time employees trying to find them. “With Symantec, we devote less than one percent of staff time to preventing and mitigating the effects of malicious code,” says Bill Engel, workstation coordinator. “And that’s dropped even further since getting the Symantec network security

Kettering Medical Center Network — Symantec Security Solutions



assessment.” Adds Burritt: “Symantec’s intrusion detection appliances, Managed Security Services, and DeepSight Alert Services and Threat Management Services save us \$200,000 a year in staff time.”

“In addition,” says Kristie Tolliver, network coordinator, “we can now use those staff resources for tasks far more valuable than routine log checking. They can focus on activities that benefit patient care more directly.”

A clear improvement in security

A before-and-after story shows the value of Symantec solutions. In early 2003, the Slammer worm paralyzed many business servers around the world. KMCN, however, had installed the appropriate Microsoft server patches, and avoided damage. But weeks later, KMCN was knocked off the Internet. A team of five IT staff spent most of a day troubleshooting to locate the cause: A server had been recently rebuilt by a staff member who had forgotten to update the patches. “We lost thousands of dollars in staff time finding and fixing this,” Burritt estimates, “and easily tens of thousands of dollars on an organization-wide level, because of lost access to the Internet.”

In contrast, in August 2005, after the Symantec security assessment, the Zotob worm began to infect Windows 2000 servers worldwide. It landed in two machines that, although outside the Kettering network, were nevertheless connected. “The person taking care of those machines had not updated the patches,” George Bohlen says. “Symantec Managed Security Services spotted the infection, notified us, and we were able to shut those machines down and repair them. Zotob never got inside our network. You can’t quantify the benefit from Symantec in situations like this, but it’s substantial.”

Adds workstation coordinator Bill Engel: “Because of Symantec, our workstation team has peace of mind that malicious code threats are well-handled. We can focus more on our other challenges.”

Fast track to compliance

Another area where Symantec helps lower costs is in complying with HIPAA. Symantec Enterprise Security Manager™ gives KMCN a fast, cost-effective way to define, measure, and report on the compliance of its information systems against internal security policies and HIPAA regulations—all from a single console. “We can analyze compliance for the entire organization,” says George Bohlen, “or drill down to a facility or department level, or even down to a critical system.”

Symantec Enterprise Security Manager gives KMCN templates for quickly configuring and analyzing systems and servers. The templates reflect extensive Symantec experience in complying with HIPAA and other regulations, as well as best practices in security. “It would be cost-prohibitive to try to cover this ground on our own,” says Burritt.

Maintaining security on servers

A challenge for the KMCN team is that any time someone alters a server, which happens often, the server must be rechecked for security compliance. “At KMCN we work with 120 IT vendors,” Burritt says. “Many of them have responsibility for the code in their applications. They make changes our IT team doesn’t know about that can compromise security.”

Adds George Bohlen: “To check our 200 servers for compliance once took about three to four days. Symantec Enterprise Security Manager cut that to half a day, saving us \$18,000 a year in staff time that we can put to more valuable uses.”

“Just the other day,” Burritt adds, “Symantec Enterprise Security Manager spotted a cluster of generic user accounts that a vendor had created in his application that compromised security. We had the vendor go back and delete them.”

Deploying 50 percent faster

“We cut 50 percent off our deployment time for Enterprise Security Manager thanks largely to help from Symantec Consulting,” says Bohlen. “And Symantec Education Services showed us how to get the most value from the product with a good class on administration.”

“But I’d say the single biggest difference that Symantec Consulting made,” says Burritt, “is with their network vulnerability assessment. We needed their outside expertise, gained from dealing with dozens of hospitals and hundreds of other organizations. Their most valuable contribution was in showing us the efficiencies and savings we’d get by teaming our Symantec intrusion prevention appliances with Symantec’s DeepSight Alert Services, DeepSight Threat Management Services, and Managed Security Services.

“Our Symantec representative, John Bourjaily, has been devoted to our organization and to providing it with the most secure environment possible,” says Burritt. “Kudos to him for the great teamwork between Kettering and Symantec.”

Licensing savings are rewarding

Part of that teamwork is the Symantec Value Licensing program, enabling KMCN to enjoy a streamlined pricing structure for their Symantec software purchases, along with upgrade protection, technical support, and volume discounts.

BUSINESS VALUE AND TECHNICAL BENEFITS

Cost Savings

- \$200,000 in staff time saved annually through firewall monitoring from Symantec Managed Security Services
- \$18,000 saved annually by reducing staff time for a security review of KMCN's 200 servers
- \$140,000 one time and \$70,000 annual savings on licensing, and \$4,000 annual administrative savings from Symantec Value Licensing Program

Return on Investment

- 100% ROI on Symantec security solutions in a few weeks, given risks averted

Time to Deployment

- 50% faster deployment of Symantec Enterprise Security Manager due to Symantec Consulting

Enhanced Security

- Less than one percent of staff time now involved in virus/security problem mitigation
- Zotob worm infection spotted, confined and repaired, avoiding severe losses

“Given the skill of today’s hackers, and the intense nature of today’s automated threats, I’d say that 100 percent payback for security solutions like the ones we have from Symantec is in a matter of weeks. Without them, you’d likely be out of business”

Bob Burritt

Director of Technology

Kettering Medical Center Network

“The Symantec Value Licensing program gives us \$140,000 one-time and \$70,000 annual license savings, along with trimming \$4,000 in yearly administrative time on purchasing and licensing issues,” Burritt says.

Prevention helps yield enormous returns

Adds Burritt: “Given the skill of today’s hackers, and the intense nature of today’s automated threats, I’d say that 100 percent payback for our Symantec security solution is in a matter of weeks. Without a sound security strategy, our organization would likely be out of business.”

But KMCN’s solutions from Symantec are helping to provide more than intrusion prevention and cost savings. They also enable the staff to focus on more valuable initiatives, such as KMCN’s recent development of a Simple Sign On application. “As KMCN physicians and clinical staff move among workstations, they have

to sign on to secure applications about ten times a day on average,” Burritt explains. “That previously took about two minutes each time. The Simple Sign On project will reduce those two minutes to 10 seconds.”

The minutes saved translate into enormous savings: Multiplied by 5,000 users who sign on ten times a day, and KMCN is gaining as many as 1,500 hours every day that KMCN professionals can devote to care rather than keystrokes.

For Bob Burritt and team, it’s just the kind of healthy difference they most want to make.