

Danbury Hospital

Giving Hospital Infrastructure a Clean Bill of Health
with Symantec Managed Security Services

Noticing increasingly sophisticated attacks against its network, Danbury Hospital, a large Connecticut medical center, out-tasked its IT security monitoring and device management functions to Symantec™ Managed Security Services. Symantec now monitors and manages the hospital's diverse security infrastructure from its worldwide network of Security Operations Centers. This solution has streamlined security response, reduced the time needed to investigate threats by 93 percent, and strengthened compliance with HIPAA and other regulations. It also allowed IT staff to focus on developing better controls to protect patient confidentiality while giving medical professionals and their patients access to critical medical information.

Securing the perimeter

The ability to combine early detection with top-of-the line care can be a key component in the fight against illness and disease. Residents of Danbury, Connecticut and nearby New York State find this health-saving combination of capabilities at the nationally-recognized Danbury Hospital (Danbury). Named in Solucient's 2004 report of the nation's top 100 hospitals¹, this 371-bed regional medical center offers better patient safety, shorter hospitalization, and a lower mortality rate than most other U.S. hospitals.

In order to provide the best patient care possible, Danbury relies on maintaining a continuous flow of information. In addition, maintaining patient confidentiality and compliance with regulations are top priorities of the hospital. With more than 3,000 employees, including 500 physicians, and thousands of patients requiring online access, retaining secure control of information was a concern.

Growing demand for health care and rising costs prompted Danbury to utilize third-party application services from Cerner Corporation and Siemens Medical Solutions. Transferring this data via the Internet to healthcare partners, the hospital faced the increasing risk of hacker attacks compromising patient confidentiality. For Rob Simon, group leader for Danbury's IT security team, this concern overshadowed the rest of his group's duties.

“Hiring more staff for a 24x7 immediate response team would have greatly increased our staffing costs. But with Symantec's global Security Operations Center providing constant surveillance, we can respond to threats quickly, no matter when they occur.”

Rob Simon

Group Leader
Danbury Hospital

Organization Profile

Danbury Hospital, www.danburyhospital.org, is a regional medical center serving residents of Connecticut and New York. It is ranked among the nation's 100 Top Hospitals® by Solucient, a leading national source of healthcare business intelligence.

Industry

Healthcare

Solution

Security Monitoring and Management

¹ www.danburyhospital.org/frontpage

Symantec's Security Operations Center provides comprehensive security monitoring to reduce unnecessary investigations and research, streamlining overall security operations.

Mobilizing the forces

“To keep our patients' private information safe, we out-tasked security monitoring to a third-party vendor in 2003,” Simon explains. “However, the company didn't provide a complete service. It just compiled unfiltered logs of all the threats possibly headed our way. My team had to sift through stacks of paper trying to determine if there were any viable threats. As a small group, we didn't have the resources to devote that much time to security, and I was concerned that we might miss something. As the threats started to evolve, we decided it was time for us to evolve as well.”

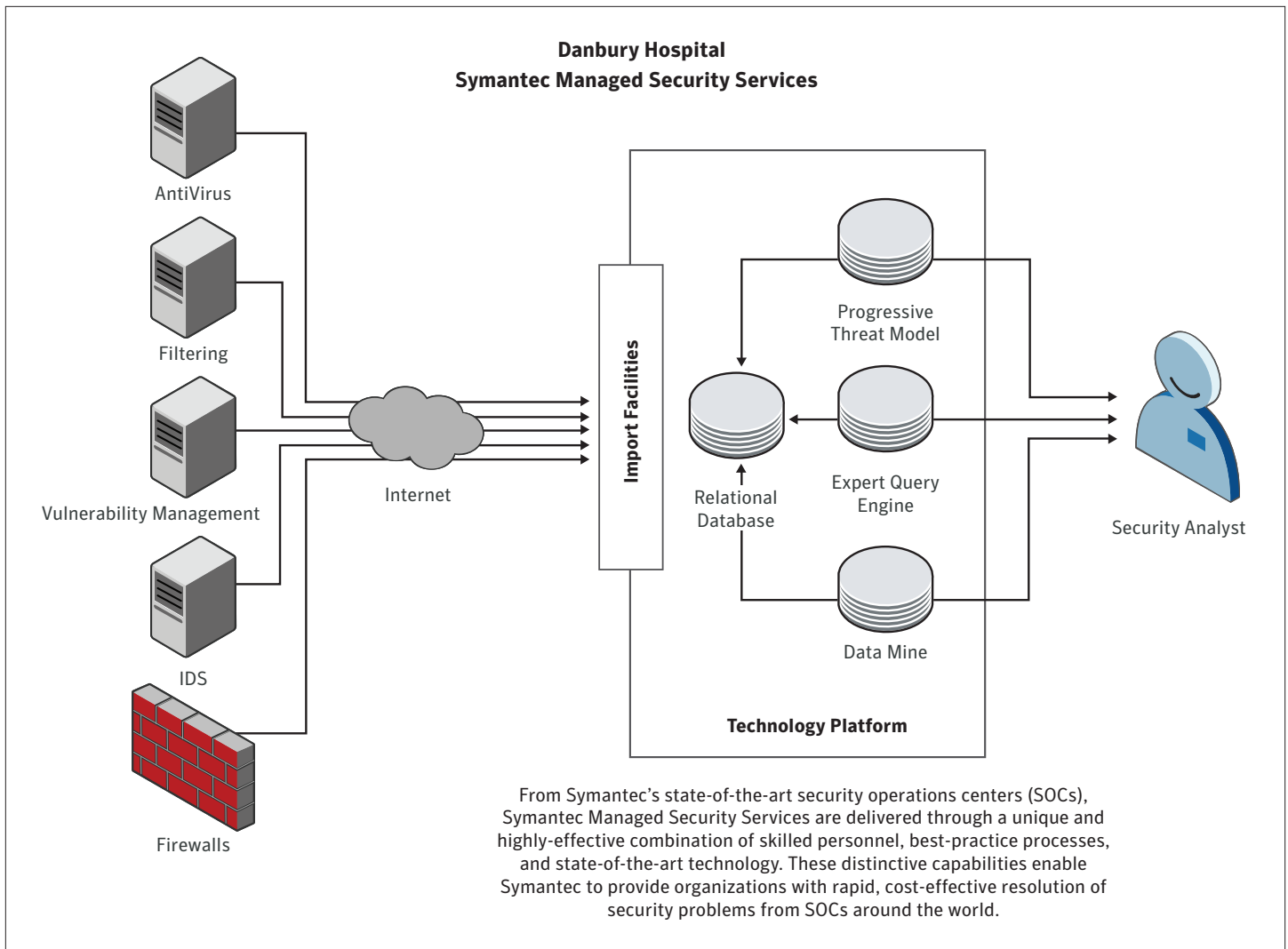
Seeking another company to manage its security, Danbury developed a comprehensive test, assessing competitors according to their ability

to identify and define threats, provide around-the-clock surveillance, monitor a heterogeneous network, and function in a vendor-neutral environment.

A leader in providing remote security solutions across multiple platforms while supporting third-party applications, Symantec™ Managed Security Services (MSS) won the business in January 2004.

Vigilant surveillance brings peace of mind

More than two years later, Danbury remains pleased with the results. “Symantec Managed Security Services is increasing our knowledge tremendously,” states Simon. “It filters the thousands of threat attempts against us and classifies them in an easily



understood format. My team used to spend four hours a day researching threats. Now it only takes a few minutes to review pertinent data, saving significant costs in administrative time alone. Plus, the functional burden of identifying threats has shifted away from us. Symantec MSS employs a global overview of potential threats, so it knows what's out there and how that affects our specific business and infrastructure.”

Choosing best-of-breed products, the hospital's security infrastructure is comprised of two intrusion detection systems (IDS), Symantec Host IDS and Enterasys Dragon network IDS; and a variety of firewalls, including Check Point FireWall-1. The Symantec Security Operations Center (SOC) in Alexandria, Virginia—one of four Symantec SOC's globally—monitors the traffic at these multiple levels of security.

The hospital's healthcare-specific applications utilize unique ports, enabling hackers to easily recognize Danbury as a medical institution and attack through the identified connections. Symantec Managed Security Services spots these threats and notifies the hospital to take suggested precautions. If the notification is merely recognizing possible problems or developing patterns, the SOC contacts the hospital via a personalized Web portal and solution-specific email messages. When the software detects potentially critical threats, an SOC technical expert calls the Danbury point-of-contact, explains the situation, and recommends solutions.

This is an important feature for the hospital. “We only staff for onsite security coverage during normal business hours,” says Simon. “Hiring more staff for a 24x7 immediate response team would have greatly increased our staffing costs. But with Symantec's global Security Operations Center providing constant surveillance, we can respond to threats quickly, no

SOLUTION AT A GLANCE

Business Drivers

- Minimize IT spending as part of overall hospital cost-containment initiative
- Comply with HIPAA and other relevant regulations
- Ensure high level of security for sensitive patient information
- Focus technical resources on high-value projects aligned with hospital's core mission

Technology Challenges

- Manage a heterogeneous security environment made up of best-of-breed components
- Move to a proactive stance for network security
- Filter thousands of possible threats to identify the most critical
- Ensure that firewall rules are tuned for optimum network performance and security

Solution

- Security infrastructure built with best-of-breed products, including Symantec solutions; out-tasked security monitoring and management to Symantec

Symantec Products

- Symantec™ Host IDS

Technology Environment

- Applications: Cerner, Siemens, Microsoft Exchange Server
- Security: Check Point FireWall-1, Enterasys Dragon, Symantec Host IDS

Symantec Services

- Symantec™ Managed Security Services

matter when they occur. It provides a level of confidence and peace that I can't begin to measure.”

Honing the rules for HIPAA

Brenda Plaag, chief privacy officer at Danbury, is responsible for maintaining regulatory compliance and internal privacy standards. She finds the integration of the security features with Symantec MSS is a tangible safeguard measure for HIPAA regulators and helps her demonstrate the hospital's compliance.

“Symantec Managed Security Services consolidated the existing rule base of our multiple firewalls, tuning the rules for tighter control,” says Plaag. “This gives us solid, statistical evidence of the difference between our security

“Thanks to the way that Symantec Managed Security Services filters threats, we only have to respond personally to one or two attacks a month, compared to up to 60 with our previous security vendor.”

Susan Fronapfel

Manager of Information Technology and Security
Danbury Hospital

BUSINESS VALUE AND TECHNICAL BENEFITS

Network Security

- No significant penetration of network since start of Symantec security management

Compliance

- Full HIPAA compliance, partially due to Symantec Managed Security Services

Staff Productivity

- 93% reduction in threats requiring staff attention (from 60 to 2 per month)
- Four hours per day previously spent reviewing threat logs, now devoted to more strategic tasks

Cost Avoidance

- Significant costs for in-house security experts to provide around-the-clock monitoring avoided

“Thanks to Symantec Managed Security Services, our security infrastructure is rock-solid, allowing us to focus on the real issue—improving our ability to better care for our patients.”

Rob Simon
Group Leader
Danbury Hospital

coverage before and after intervention by Symantec. This shows our commitment to complying with HIPAA whenever we can.”

“A continuous supporter of our compliance efforts, Symantec Managed Security Services directed its Solutions Enablement branch to conduct a security audit of our firewall rules. The audit evaluated the current effectiveness of our rules and recommended specific changes. This allowed us to pinpoint actual dangers and strengthen our security environment. In addition, the skills transfer from the Symantec team is increasing our staff's knowledge to the point where we can fine-tune our own firewall rules without help.”

Ongoing security protection and improvement

Symantec MSS is instrumental in decreasing the security workload of Danbury's IT staff. “Thanks to the way Symantec Managed Security Services filters threats, we only have to respond personally to one or two attacks a

month, compared to up to 60 with our previous security vendor,” explains Susan Fronapfel, manager of information technology and security for Danbury. That's a 93 percent reduction in incidents requiring staff time.

That benefits not just the IT team, but hospital employees—and patients—as well. “More time for our IT staff means that we can focus on other areas, such as the email system and online billing, to improve hospital operations,” says Fronapfel. “It also means better care for our patients. We're in the process of integrating new backup and redundancy equipment into our network to ensure our patients' protection and the accuracy of our information.”

Taking care of business

With Symantec Managed Security Services providing early detection and top-of-the line care, Danbury's security infrastructure remains healthy. Although it continues to be alert to the increasing sophistication of technological attacks focused on healthcare providers, the hospital is no longer in a

continuous reaction mode against threats. Currently, the security team is moving to more proactive measures, beginning with network forensics, which involves investigating network events to pinpoint attack sources.

“The hospital deals with life-threatening emergencies on a daily basis,” concludes Simon. “Security breaches are the last thing we have time for. However, with the amount of information we get and the threats we face, there is the potential for serious problems. Thanks to Symantec Managed Security Services, our security infrastructure is rock-solid, allowing us to focus on the real issue—improving our ability to better care for our patients.” ■