

### Situation

Serving over 250,000 patients annually, Caritas Christi Health Care is the second largest health care system in New England. Caritas Christi is headquartered in Massachusetts and has two medical centers, four hospitals and remote doctor's offices that need to share data both internally and externally using the Internet and Web-based email. With a distributed network of more than 5,500 medical employees using Web-based email and the Internet regularly, Caritas Christi needed to maintain Health Insurance Portability and Accountability Act (HIPAA) compliance to protect patient data privacy, secure computer network traffic and safeguard electronic healthcare transactions.



In addition to maintaining HIPAA compliance, Caritas Christi's IT department also needed a solution to curtail its users from downloading malicious content via the Web and to control the traffic that is allowed to enter its internal network. Furthermore, recent Internet threats such as Bagle and MyDoom made it clear that a robust network security solution that would not slow its Gigabit speed network performance, including high performance antivirus scanning, was necessary to protect its health care system's sensitive patient data.

### Solution

Being an open source shop, Caritas Christi had a unique set of criteria during their search for a more robust security solution. Their initial research for a solution to safeguard Internet use and Webmail had the company testing open source antivirus and Web content filtering software but these products were not as powerful as the health care's network required. Caritas Christi then decided that a security appliance integrating several security applications such as antivirus and content filtering would better fit its needs for bandwidth and performance. After reviewing products from Blue Coat, Trend Micro and Webwasher it became clear to Caritas Christi decision makers that, while they needed a comprehensive solution, they required a solution that did not hold them to a certain number of users.

**Deployment:**  
FortiGate-800  
FortiGate-60  
FortiGate-50A

**Industry:**  
Healthcare

Caritas Christi began testing Fortinet's FortiGate® ASIC-accelerated network security platform and liked the fact that the antivirus scanning worked extremely well while other key security features such as firewall, virtual private network (VPN), content filtering and intrusion detection and prevention (IDP) were running. In addition, the FortiGate systems provide an entire network security solution at a cost per hardware platform, not per user. "Because our user base fluctuates, it doesn't make sense to buy a solution that charges per user – it is a waste of money," said Tavares Marsh, Security Engineer for Caritas Christi Health Care Systems. "We chose Fortinet's FortiGate Systems because we get all of the security functionality we need and the performance that we require without worrying about how many users are behind it."

To secure more than 5,500 users' Webmail and Internet use, Caritas Christi deployed Fortinet's network security platforms. The company deployed two FortiGate-800 enterprise-class systems - one at headquarters in the core data center running antivirus to scan all Internet traffic. The companion platform resides inside a hospital, and connects back to the data center to protect the health care system's data running through virtual local area networks (VLANs) for essential Federal Drug Administration (FDA) and vendor device communications. This second FortiGate-800 system is also being used for intrusion detection and prevention (IDP), antivirus, and security policy enforcement. Eight FortiGate-50A systems have been deployed in remote doctors' offices, providing secure virtual private network (VPN) connections back to the core data center. A FortiGate-60 system has been deployed at the backup Internet connection running antivirus to scan all backup Internet traffic.

Caritas Christi's FortiGate systems receive automatic updates for antivirus signatures via Fortinet's global FortiProtect™ Network as well as Web content filtering in all locations to control Web access. The FortiGate platforms help the health care provider maintain HIPAA compliance and deliver Complete Content Protection through the integration of a broad range of cost-effective security functions in real-time -- including antivirus, firewall, VPN, IDP, content filtering, traffic shaping, spyware protection and anti-spam.



## Success

"We are pleased with our decision to choose Fortinet because the FortiGate systems provide all of the security functions we need to safeguard our online data in a single security platform," said Marsh. "Fortinet's FortiGate systems provide a complete network security platform that performs impressively while all of the security features are turned on. All of the Internet problem areas around the hospitals such as remote offices and connections to vendor systems are now protected from network damage in a very cost-effective way."

## About Fortinet

Fortinet is the pioneer and leading provider of ASIC-accelerated unified threat management, or UTM, security systems, which are used by enterprises and service providers to increase their security while reducing total operating costs. Fortinet solutions were built from the ground up to integrate multiple levels of security protection--including firewall, antivirus, intrusion prevention, VPN, spyware prevention and anti-spam -- designed to help customers protect against network and content level threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified in six programs by ICSA Labs: (Firewall, Antivirus, IPSec, SSL, Network IPS and Anti-Spam). Fortinet is privately held and based in Sunnyvale, California.

CAS127-0507

