

Financial Medical Systems Case Study

A SonicWALL Success Story



Employing one of the region's largest private medical billing teams, Financial Medical Systems performs billing and follow-up activities for over 1,000 hospital-based physicians and independent practitioners. They faced the challenge of tightening security for an increasingly open sensitive network.

"Our network is geared around security," said Ralph Marra, CIO of FMS. "Because we deal with confidential medical and identity information on a daily basis, we have to guarantee it's safe. That means we need to fully comply with PCI and HIPAA regulations.

"Previously, FMS was more concerned about inside-out security, making sure any data going out was encrypted and couldn't be captured or tagged. The legacy Cisco firewalls they had when I came on were relatively wide open. Once we started transacting over the Internet, we automatically had an outside-in issue with malware. Another big problem we've faced was e-mail attacks. We had to clean viruses off nearly one in ten desktops because people opened e-mail that they shouldn't have."



The EX-1600 detects the identity and security state of remote devices, protects against unauthorized access by enforcing granular policy and connects users seamlessly to mission-critical enterprise resources.

The SonicWALL Solution

To secure his network at the gateway, Marra chose paired SonicWALL E-Class NSA E6500 network security appliances configured in high availability mode. For secure remote access, he selected SonicWALL Aventail E-Class EX-1600 SSL VPN appliances, also in high availability. To establish e-mail security, Marra added a SonicWALL E-mail Security 300 appliance.

The Results

"Recently, a client insisted they were sending us files, but we weren't getting them," said Marra. "We found out the new E6500 had blocked the files because they were all infected with viruses." Combining multi-core processor technology and a re-assembly free deep packet inspection engine, the E-Class NSA E6500 appliances provide FMS with high-speed intrusion prevention,

anti-virus, anti-spyware and application firewall, with application-level control.

"We now have about 40 people remotely accessing resources over the SSL VPN," said Marra. "They get authorized on before they even go through the E6500.

"The beauty of it is we can see who logged in when to access what specific resources. It's a great reporting tool." The award-winning EX-1600 allows FMS to detect the identity and security state of remote devices, protect against unauthorized access by enforcing granular policy and connect users seamlessly to mission-critical enterprise resources, giving FMS optimal return on its technology investment.

"Our productivity on the e-mail side has gone up dramatically," said Marra. "The spam solution is phenomenal. Now nobody worries about it." The SonicWALL ES 300 provides FMS with powerful protection against inbound spam, phishing, viruses, Denial-of-Service, Directory Harvest and Zombie attacks, while preventing outbound leaks of confidential information and violations of regulatory compliance laws.

"When you add up the security, the interface, the ease of integrating a full solution—one-stop shopping with our systems integrator and SonicWALL was the best thing we could have done," said Marra.



SARCOM partners with SonicWALL to provide you with comprehensive security for your business. Call your SARCOM Account Executive today to discover a complete solution for your organization.