

Moffitt Cancer Centers simplifies e-mail security with Secure Computing IronMail

MOFFITT CANCER CENTER AT-A GLANCE

Industry: Healthcare

Location: Tampa, FL

Business needs: Simplify messaging security to stop spam and grueling e-mail security management tasks

Solution: Secure Computing's award-winning IronMail

Results

- ◆ Simple installation process, backed by "awesome" support
- ◆ Unique "spam cocktail" and multi-identity reputation system delivers the accuracy needed to eliminate false-positives
- ◆ CIO named IronMail one of the year's major IT successes
- ◆ Reporting eliminated the need to enlist Exchange administrators for routine inquiries
- ◆ Reduced administration time spent of managing messaging security from 30 hours per week to less than two hours per week

"Switching to IronMail was like night and day. Users noted immediately that CipherTrust's solution was not blocking legitimate e-mail, and they love the quarantine function. Now they can focus on the important research work and less on the distraction of spam.

*DONALD WASYLNA,
INFORMATION SECURITY
OFFICER, MOFFITT CANCER
CENTER*

Secure Computing Corporation

Corporate Headquarters
4810 Harwood Road
San Jose, CA 95124 USA
Tel: +1.800.379.4944
Tel: +1.408.979.6100
Fax: +1.408.979.9501

European Headquarters:
Tel: +44.0.870.460.4766
Fax: +44.0.870.460.4767

Asia/Pacific Headquarters:
Tel: +852.2520.2422
Fax: +852.2587.1333

Japan Headquarters:
Tel: +81.3.5339.6310
Fax: +81.3.4496.4537

For a complete listing of all our global offices, see www.securecomputing.com/goto/global/offices

IronMail delivers unique combination of powerful messaging security, simplified administration and "awesome" support

H. Lee Moffitt Cancer Center & Research Institute at the University of South Florida is part of an elite group of National Cancer Institute Comprehensive Cancer centers, focused on research aimed at the rapid translation of scientific discoveries to benefit patient care. This not-for-profit institution records more than 135,000 visits per year and has 3,500 e-mail users on the Microsoft Exchange and Outlook platforms. The research institute receives about 20,000 e-mails per day.

Business challenge

Increasing spam was the crux of Moffitt Cancer Center's challenges. Initially, to solve the problem, the Center deployed MailScan, but that solution did not meet the needs of the administration team, or the demands of end users who required that the unwanted messages be eliminated from their system. .

"We simply had too many complaints and unhappy users who struggled with junk mail features and were still getting tremendous amounts of spam and unsolicited commercial e-mail," said Donald Wasylyna, Information Security Officer for Moffitt Cancer Center. "And we were spending an outrageous 20 to 30 man hours a week dealing with complex rule sets and other management functions. It simply wasn't working, and more and more calls came into the help desk. Spam was clearly affecting the productivity of our researchers and employees."

Additionally, as a teaching hospital it was important to Moffitt that they were able to receive messages that contained words such as 'Viagra' or parts of human anatomy, which might be a part of legitimate message traffic. To do that, the Center needed a solution that had granular policy controls and settings with which they could customize spam filtering options.

Why Moffitt Cancer Center selected Secure Computing

After evaluating solutions such as MailScan, Tumbleweed and Symantec, Moffitt decided to purchase Secure Computing's IronMail to help eliminate spam. At the same time, IronMail would enable the Center to set rules and policies that ensure all legitimate mail makes it through, despite some of the words that might be included.

Moffitt turned to Secure Computing for its leadership in messaging security—and unique combination of powerful technology that could understand the difference between legitimate mail on human anatomy and medications—and spam. In addition, simple quarantines and automation could dramatically reduce the daily burdens on users struggling with manual junk mail filters.

Results

Secure Computing's award-winning IronMail appliance instantly found that more than 75 percent of incoming e-mail was spam, and stopped it at the gateway. The appliance also delivered the intelligence needed to understand appropriate terms and let legitimate medical e-mail through. With a simple set of e-mail instructions, users migrated to the IronMail solution with no problems.

"Default rules made for simple installation that was backed by awesome Secure Computing support," said Wasylyna. "IronMail is not blocking legitimate medical e-mail and end-users love the quarantine function, which quickly notifies the end-users and eliminates all of the false positives we were experiencing with our previous solution."

With IronMail, administrators that used to spend up to 30 hours per week struggling with spam now spend just two hours a week proactively taking advantage of IronMail's wealth of features and flexibility to easily create custom hands-on rules that fit the unique needs of medical researchers.

"The IronMail reporting is so good that we are able to do all kinds of new Exchange troubleshooting that would normally require us to enlist our Exchange system administrators. We don't need to call them any more," said Wasylyna.