

Riverside Health Care System

Riverside Health Care System, Inc, located in Southern Westchester County, New York, includes: St. John's Riverside Hospital -Andrus and ParkCare Pavilions, the Community Hospital at Dobbs Ferry, Cochran School of Nursing and the Michael N. Malotz Skilled Nursing Pavilion, Valentine Lane Family Practice, and Park Central Sports Medicine and Rehabilitation Center.



Key Features of Enterprise Edition

- **Time Zero Virus Technology™:**
Only solution available to combine Avinti, Kaspersky, and McAfee
- **Sender ID Authentication & MailFrontier Reputation™:**
Latest industry standards already included
- **Bayesian Fraud Filtering:**
Market-leading anti-fraud solution
- **One-screen Quick Configuration:**
Under one hour to threat-free email
- **Upgrade Auto-Download:**
Signature and engine updates made automatically available
- **Enhanced reporting: More robust analysis of solution ROI**

Challenge: Seeking a cure for spam-related complications

With six clinical facilities, over 300 physicians, and over 2500 employees, Riverside Health Care System represents one of the largest systems in the managed care community of New York. And with over half of its healthcare staff on email—in every area and at all hours—effective email communication is essential to smooth round-the-clock operations and quality patient care. Offers Niall Pariag, Senior Network Administrator for Riverside Health Care, "Every employee of this hospital depends on email—which means that in a way, our patients do as well. And because we recognize its importance, we take email management and security very seriously."

Riverside Health Care implemented email security almost simultaneously with the implementation of email itself, but by late 2003, it was clear that spam volume was outstripping the solution—and the best efforts of the IT team to keep up. Pariag reports that Riverside Health Care unwanted email volume well exceeded 80 percent of all mail received—and its content filter-based solution was catching only about 70 percent of that unwanted mail.

Even more dismaying was the high false positive rate—Pariag and the IT staff spent significant time every day dealing with misidentified email complaints and helping users retrieve "lost" email from quarantine. "Spam fighting, tracking, and managing easily represented 10 percent of our job," states Pariag.

With a content filter of borderline effectiveness and increasing burden, Pariag began a search for a replacement email security solution. What confronted him on the market was a range of look-alike solutions in every form—third generation products that all seemed to promise effectiveness and accuracy, easy administration, and a full range of protection modules including anti-virus options.

"The latest range of email security products looks so similar at first glance that it was hard to know where to start," remembers Pariag. "So what I used as an immediate differentiator was how quickly vendors responded to me and helped me get the product into trial. I figured that the easier they made it for me to evaluate their solution, the more serious they were about having me as a customer."

Solution: MailFrontier Gateway Server™, Enterprise Edition

After looking at various products and form factors, Pariag opted for an email security solution in application form. Price was a key factor, but ease of deployment also played a part in his decision. "Simply put," Pariag notes, "two vendors could get me up on their solution fastest. So I started with them."

MailFrontier Gateway Server was one of the two applications on Pariag's shortlist. "Before I began my evaluation, I felt certain I was reviewing two very similar solutions," he says. The trial process showed Pariag that all applications are not created equal:

Ease of Installation: One application had a particularly involved configuration process. "It was long and complex and in the end, still required me to perform additional modifications to my email server in order to work. MailFrontier, on the other hand, was set in five steps because the product already integrates some key technical controls to make life easier for the administrator. From the start, MailFrontier delivered the more well-thought out product," comments Pariag.

"When first looking at new anti-spam options, I thought the search for a replacement of my current solution would take forever. What made MailFrontier stand out was how quick and easy it was to download the product and trial it. Immediate results keep MailFrontier products ahead."

Niall Pariag
Senior Network Administrator
Riverside Health Care

Why MailFrontier

- **Effective:** MailFrontier stops 98 percent of unwanted email at network perimeter
- **Easy:** MailFrontier requires just 10 minutes a week to manage
- **A Step Ahead:** MailFrontier continues to evolve its technology and its techniques to stop new threats as they emerge

MailFrontier

MailFrontier is an email security company trusted by organizations to protect their email from spam, virus, phishing, fraud, and other dangerous and costly email threats. In a world where email threat evolves daily, only MailFrontier promises to be effective, easy, and a step ahead for its customers and their users.

Ease of Integration: Like many IT administrators, Pariag has spent significant time creating an LDAP directory to manage and organize users. So he was thrilled that both solutions offered LDAP integration. But what he found was that the two applications had different definitions of integration. "On one hand, the LDAP integration feature was not at all elegant—and there were errors I had to fix. Updating also came with issues for me. But MailFrontier handles LDAP integration like they own the concept—and in a way, they do. No problems, no errors, no issues," Pariag notes

Ease of Management: Moving on to the actual trial period, the other application required Pariag to call support numerous times to get the trial running properly. "While I was getting answers to my questions, I was left wondering if I'd be this dependant on the support staff as a customer. Would I be trading time on the phone talking to unhappy users for time on hold waiting for support?"

The MailFrontier trial offers a completely opposite experience. "After I got the trial license, I had the solution live and working in less than an hour," Pariag states. "In fact, I thought it was too easy. For almost the entire trial period, I was in denial that the solution was performing so well without any blood, sweat, or tears from me." Finally unable to resist second-guessing the trial results, Pariag called MailFrontier support to check his work. The MailFrontier support technician confirmed all of Pariag's settings and offered just one helpful fine-tuning suggestion. "He asked me to click one button—and suddenly it was working even better."

Results: A solution that saves time, spares users, and stops spam

Easy as MailFrontier is for Pariag to manage, he still needed to ensure that the solution fulfilled its primary function: stopping spam. As it turned out, there was no need for compromise—the trial results showed that MailFrontier could deliver effectiveness and accuracy as well as administrative ease. Since full implementation, results include:

- **Effectiveness reported at 95 percent with almost 100 percent filtering accuracy**
- **Spam management time reduced to less than 5 minutes a week**
- **False positive calls reduced to under one a week**
- **Up to 300 viruses blocked per day**

Pariag has received much praise for his implementation of MailFrontier, but one overhead comment is especially memorable to him. "The day the solution went live, people noticed—even though I hadn't said anything yet. Specifically, our CEO was heard to say, "I don't know what Niall did—but it worked."

“MailFrontier told me that I would spend less than 10 minutes a week managing spam after installing MailFrontier Gateway Server. They were wrong. I only spend five.”

Niall Pariag
Senior Network Administrator
Riverside Health Care System



1841 Page Mill Road
Palo Alto, CA 94304
866-3NO-SPAM