

The True Story of How a Simple Appliance Transformed Angry Email Users into Delighted Customers, Cured an ISP Supervisor's Headache and Protected a Big Fish in a Big Pond

Manuel Miranda had a headache.

For most people, Puerto Rico and the Caribbean islands are a tropical paradise of white sandy beaches, crystal blue seas, swaying palm trees and romance. For Manuel, the area was a snakepit of deception, lies and unwelcomed intruders.

Miranda is ISP supervisor for WorldNet Telecommunications, Inc. and, like most ISP supervisors, he was trying to accommodate email users (both business and personal) who wanted him to do something about spam and viruses. Like email users worldwide, they were upset at the wasted hours they spent unclogging email accounts that, in some instances, were 90 percent spam.

Users received regular spam, image spam, PDF spam, Excel spam, “pump and dump” spam and pornographic spam. There were viruses, worms and Trojan horses.

And Miranda was responsible for getting rid of all of it.

The Company: WorldNet Telecommunications, Inc.

WorldNet is a big fish in a big pond: the Caribbean region. Established in 1996, it is the only 100% Puerto Rican-owned local telecommunications company. Over the past decade the company has grown from a traditional supplier of telephone services with 10 employees into a modern telecommunications facility with over 180 employees.

Their mission is to satisfy the specific telecommunications needs of local industries that include pharmaceuticals, manufacturing, hospitality and government and well as small businesses and home users.

Over the past decade WorldNet has experienced steady growth by offering customers one-stop shopping for “concierge” telecom services including voice services (zone, local and long distance), Internet services (including VoIP and high-speed web hosting), electronic billing and telecommunications consulting. They have the capability of providing a single Internet home connection or evaluating, implementing, servicing and maintaining a complete world-class corporate telecommunications solution for their 6,000 customers.

WorldNet attributes its growth and success to rapidly responding to clients' requests. And that was why Manuel Miranda had a headache.

The Problem: Death by clogging

Recently, WorldNet began offering ISP services—including a Linux-based mail server running on a Sun Solaris using a Java Enterprise system—and almost immediately spam began strangling their mail server. Customers found themselves spending more time eliminating unwanted email than in answering legitimate email—assuming they could even find it. Moreover, all that spam was residing on WorldNet’s email server, consuming up to 40% of the company’s storage space.

In addition, Manuel Miranda had to combat the proliferation of new viruses and worms that, in some instances, threatened to shut down corporate servers. By the time filters were developed to prevent these viruses and worms, it was too late; the system was already infected.

Miranda recognized that the problem he faced was beyond the capabilities of most software security solutions, so he began evaluating security appliances.

“I decided on an email security appliance because it was the best solution for us,” Miranda revealed. “We required something that stopped spam and viruses in their tracks. That requires advanced features like zero-hour protection and pattern recognition—features that the software programs I evaluated didn’t offer.

“This level of protection doesn’t come cheap. I looked at the industry leaders—the brands I expected would solve the problem—and, indeed, they were very costly. Then I heard about Mail-SeCure from PineApp. It offered everything I wanted for about half the price. Naturally I was a little suspicious because this seemed too good to be true.

“I accepted the Mail-SeCure free 30-day trial because they guaranteed my satisfaction and they offered free tech support. Basically I had nothing to lose.”

The Solution: Mail-SeCure Total Perimeter Security

Mail-SeCure is attached outside the network, so it blocks spam and viruses *before* they ever enter the network. Because spam is quarantined offline, it frees up valuable network storage space.

Right out of the box, Mail-SeCure blocked 95% of WorldNet’s spam and viruses.

“Installation was very easy,” Miranda recalled. “Because we’re an ISP, we spent a couple of hours fine tuning the system, inserting domain names and determining rules. Fortunately, the Mail-SeCure worked with our existing rules, so that made my job easier. In fact, their entire management system simplifies my oversight responsibilities.”

When Miranda was finished, the company’s email server was working faster and more efficiently, it easily accommodated increased traffic, and the Mail-SeCure appliance was blocking over 98% of WorldNet’s spam and viruses with a false-positive rate of 1%.

“Best of all, our clients are extremely happy,” Miranda concluded. “Their productivity has soared because they no longer have to deal with spam and viruses. If, on occasion, legitimate email is blocked, it’s very easy to fix. I quickly search a list, place a checkmark, and the email is released. That’s it.”

There’s an interesting postscript to the story. One of WorldNet’s customers, a municipality ISP, was impressed with the almost total lack of spam and viruses on the company’s network. The smaller ISP asked for the specs, and when they discovered that Mail-SeCure was half the cost of the competition, they ordered one. As a result WorldNet, a Mail-SeCure client, became a PineApp’s Caribbean Mail-SeCure reseller.

About the Mail-SeCure Appliance

Mail-SeCure provides total perimeter security.

It is located outside the network, so it blocks threats like spam and viruses *before* they reach the network. It creates a buffer between the Internet and an organization's email systems by using a complete system of perimeter anti-spam/anti-virus security layers.

Mail-SeCure proactively protects networks against targeted and non-targeted email threats

The appliance includes an arsenal of 11 anti-spam engines and five anti-virus engines that proactively protects organizations and enterprises from both targeted email threats (spam, viruses, worms, Trojan horses) and non-targeted email-related threats (mail-bombing, denial of service and backscatter).

Anti-spam engines include pattern detection, zombie detection, zero-hour detection, IP reputation and image spam defense, plus a heuristic and a Bayesian engine to recognize spam in any form and block it.

Anti-virus engines include three signature based, one heuristic based and one zero-hour detection mechanism.

Mail-SeCure requires no updated filters and firmware to meet new threats

Most email security solutions require organizations to update their software or firmware to meet new threats. Since it takes time to identify new threats and find appropriate protection, companies are left vulnerable. This is especially critical considering many threats last less than a day. By the time security firms find a cure, it’s already too late.

Mail-SeCure’s anti-spam/anti-virus engines protect organizations right out of the box. For example:

- Its zero-day capabilities automatically protect a network against current and future spam, phishing and virus threats.
- Its pattern recognition analysis spots spam in any form—including image spam, PDF spam, Excel spam and other emerging threats—and blocks it.

With Mail-SeCure, organizations are automatically protected from day one.

Mail-SeCure saves network bandwidth

Unlike most competitors, Mail-SeCure is located outside the network. As a result it blocks and quarantines spam and *before* it ever reaches the network, which saves valuable bandwidth. This is especially important since image spam (PDF, JPEG, GIF, Excel) requires megabytes of storage. Reports indicate image spam now accounts for half (or more) of all spam on networks. Some companies complain that image spam is clogging their mail servers and bringing them to their knees.

Mail-Secure provides simple-to-use management tools

The appliance provides administrators with easy-to-use tools to enforce advanced local policy as well as a mechanism to control and manage mail flow, so it is also easy to set up and use almost immediately.

Mail-SeCure costs less

Many customers state they purchased a Mail-SeCure appliance and yearly license for less money than many competitors charge for the annual license alone. However, the main reason they made the purchase was that Mail-SeCure simply worked better than the others.

For more information on how Mail-SeCure can offer your company total perimeter security, visit <http://www.pineapp.com>.