telepak.net

Customer Case Study

Large ISP Deploys PineApp Mail-SeCure to Filter Spam for Thousands of Users

Spam Now Virtually Eliminated for About Half the Price of Competing Solutions

Jackson, Mississippi-based Telepak Networks, Inc. (www.telepak.net) is a large Internet service provider (ISP) providing Internet, telecommunications and network services to thousands of residential and business customers within the state.

Initially, Telepak relied on free software such as SpamAssassin to screen incoming emails for spam before pushing it out to users through their three Sun 220R servers (running Solaris). Though outwardly inexpensive, this solution required frequent updates that occupied significant amounts of administrative time. It also proved inadequate performance-wise, becoming quickly overwhelmed during spam surges and frequently misidentifying "good" emails as spam. Explains systems administrator Joseph McNealy, "We really were in a no-win situation, spending a lot of admin time without accomplishing the goal."

As time went on and volume grew to a total of two to four million emails a day, the servers became increasingly bogged down, and the situation reached a critical level. Says McNealy, "Some of our business customers were waiting days for important emails to get through the masses of spam. We were getting dangerously close to not being able to do business."

The Solution: Mail-SeCure Total Perimeter Security

Desperate for a new solution to help control spam, McNealy searched for spam appliances on Google. Although most anti-spam solutions he found seemed more appropriate for smaller-sized businesses and incapable of handling the large email volume of an ISP, he was able to identify several potential options, including appliances from Barracuda and McAfee, and the PineApp Mail-SeCure anti-spam appliance.

"The improvements have been nothing short of remarkable. The servers are no longer bogged down, and users, especially on the corporate level, couldn't be happier about the disappearance of spam from their inboxes."

Joseph McNealy,
System Administrator,
Telepak Networks

IN A BRIEF

The Customer:
Telepak Networks

The Challenge:
To find an easy to manage, cost-effective spam filtering solution capable of handling the load of a high volume ISP with two to four million daily incoming emails

The Solution:
Installation of a trio of PineApp Mail-SeCure 5080 anti-spam appliances to filter all incoming emails

While most of these solutions were comparable in functionality, the PineApp Mail-SeCure was priced significantly lower. Says McNealy, "One competitor wanted $90,000 for the same functionality, and that was before we factored in the additional $4,000-$5,000 per year per unit for yearly updates. PineApp's solution came in at about half of that, and they were even able to provide a customer reference from another high volume ISP who had successfully deployed the Mail-SeCure."

Telepak swiftly received a pair of PineApp Mail-SeCure 5080 units for evaluation. Installation required little more that an initial reconfiguration and it wasn't long until they were fully up and running, and producing immediate results. Especially impressive to McNealy was the ability to create spam policies, and the wide range of statistics visible to administrators. "We learned that over 97% of our incoming mail was spam, and have experienced only a few false positives in cases where newsletters our users had subscribed to didn't make it through."

When the evaluation period ended, Telepak purchased the units without hesitation. According to McNealy, the improvements have been nothing short of remarkable. The servers are no longer bogged down, and users, especially on the corporate level, couldn't be happier about the disappearance of spam from their inboxes. "We had some corporate users who previously received over 100 spam emails a day. Now, they get none. Our deployment of the PineApp Mail-SeCure appliances has definitely helped us retain customers that otherwise may have become fed up with the abundant spam."

Not long after Telepak's Mail-SeCure deployment, PineApp unveiled their new IP Reputation system that classifies mail from "grey" (neither a known spammer nor a known safe sender) IP addresses based on a variety of statistical analyses and flow control policies. This extra level of protection has resulted in a traffic reduction of more than 50% for Telepak.

Telepak is now rolling out a "fiber to the home" project that they project will significantly increase the number of users in the near future. If all goes as planned, they expect to purchase additional PineApp units as volume increases.

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 multi-layered anti-spam and anti-virus systems that proactively protect 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; Its zero-day capabilities automatically protect a network against current and future spam, phishing and virus threats. Moreover, 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 even *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.