Simpson Millar LLP Solicitors

Customer Case Study

Simpson Millar LLP selects PineApp's security solution to increase staff productivity

Simpson Millar LLP

Simpson Millar LLP is a national law firm with a history spanning over 100 years. As specialists in Personal Injury, a substantial part of its legal service practice is channeled from the Communication Workers Union, yet it also provides expertise to private clients across a range of areas including family law, financial services, medical negligence and employment law.

The Problem: a security net with too many holes, time to redress the balance

Email spamming techniques are much more sophisticated and virus attacks are now more frequent. Given this rise, the number of the spam emails slipping through Simpson Millar LLP's security net increased, clogging up inboxes and reducing computer performance. In light of this Simpson Millar LLP needed a solution that could protect against emerging threats both known and unknown. Jonathan Lynch, IT manager, Simpson Millar commented, "Our existing solution frequently crashed and was ineffective. We found we had to reboot ourt system several times a day. Email security is an important aspect of our IT strategy and eventually it became a drain on my time and that of everyone across the firm."

Searching for a solution

Simpson Millar LLP began searching for a more reliable and cost-effective solution to prevent email spam. Since a software option had proved ineffective the IT team decided that an appliance based, hardware system would be a better choice. "I researched several online solution systems from some of the most well-known security vendors but I remained unconvinced by their value. In fact they seemed considerably over-priced for the services they provided," added Lynch. In several instances the IT team was quoted more than £7,000 for a software package similar to its existing security protection and unsurprisingly this was viewed as far too expensive, especially when reservations remained over the reliability of the options available.

"In the challenging economic climate PineApp offered us the perfect solution that matches our business needs completely, I wouldn't hesitate in recommending it to anyone".

Jonathan Lynch,
IT Manager,
Simpson Millar LLP

IN A BRIEF

The Customer:
Simpson Millar LLP

The Challenge:
To find the simplest, best value and most effective network security provider

The Solution:
PineApp's Mail-SeCure 2040

Out with the old and in with the new

Convinced that there was a more effective provider on the market, John Wolski, network administrator, Simpson Millar LLP met the PineApp team and learnt about the company's comprehensive range of practical solutions. PineApp provided Simpson Millar LLP with a free 60 day, no contract, no hassle trial of its Mail-SeCure 2040 appliance, resulting in remarkable and immediate improvements.

Number one for customer service

Since deploying PineApp's Mail-SeCure solution, the management of Simpson Millar LLP's email security has been significantly improved. PineApp's consultative approach has also meant that they not only understand the nature of the business but could also resolve potential issues swiftly. This is evidenced by the fact that some of PineApp's senior security consultants are always available when assistance is required.

The right choice

It has now been a year since Simpson Millar LLP began using PineApp's solution and as testament to the reliability of PineApp's product there have been zero complaints. An increase in staff productivity has also been noticed. Since employees no longer need to spend time sifting through irrelevant messages or waiting for the network to be restarted they have more time to focus on their core job. An added benefit is that servers and drivers now work faster as they are no longer hit by damaging and destructive traffic.

Email security poses a serious threat to the security of any business which is why companies should invest time to find the right solution. "Security provision is not something that should be rushed into and sales people have a tendency to put a glorified spin on things. What companies often fail to realize is that many of the better known, more complex software options charge for upgrades and add-ons," Jonathan Lynch added. "In the challenging economic climate PineApp offered us the perfect solution that matches our business needs completely, I wouldn't hesitate in recommending it to anyone."

About the Mail-SeCure Appliance

Mail-SeCure 2040 appliance protects midsized businesses', of up to 250 users networks, from both targeted and non-targeted email-related threats.

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/.