

Case Study



Global Leader in IT Business Management
Irons Out its Email Security Problem

THE SITUATION

Headquartered in the UK, Touchpaper provides round-the-clock support services and software to thousands of customers around the globe. Touchpaper has more than 1,700 customers (equivalent to three million users) including financial services institutions, manufacturing businesses, retailers, central and local governments, transport, IT and utility services and professional services practices.

Touchpaper prides itself on customer satisfaction, which has helped it maintain long-standing relationships with numerous clients. Maintaining high levels of customer service requires effective and efficient communications tools such as email. Unfortunately, advances made in email technology have been accompanied by a rising tide of spam, viruses and other threats. This was beginning to impact the productivity of Touchpaper's 200 email users and the company realised it had to act now to prevent any problems impacting its own customers.



Email management and security should be automated, reliable and (most importantly for both internal and external users) invisible. They just want to know that it works and, thanks to IronPort, it does. ”

TOUCHPAPER AT A GLANCE

Email users: 200

Challenge: Prevent legitimate emails from being quarantined and ensure staff can provide support to customers without experiencing any delay

THE IRONPORT ADVANTAGE

- Email users no longer receive spam messages or have legitimate messages blocked
- Email management and security is automated and reliable
- Customer service has improved since support messages to clients no longer run the risk of being wrongly quarantined
- IT managers no longer waste time dealing with email release requests but can focus on more strategic IT tasks
- Attachments can be managed by IT according to departmental needs and types of users



TECHNICAL CHALLENGES

Although Touchpaper had an anti-spam solution in place, the software was struggling to keep up with the evolution of spam-based messaging and to separate legitimate emails from spam emails. This meant that legitimate emails would be quarantined alongside suspected viruses and spam.

Apart from the obvious inconvenience to the intended recipient and the frustrations of the sender, the IT department faced an increasing workload. Every morning, a member of the team would spend around 30 minutes trawling through the quarantined emails to identify and release legitimate messages.

Employees also had to deal with a small, but increasing, number of offensive spam messages that were passing by the existing anti-spam solution. “To tackle this problem we had to set up point solutions on PCs of the individuals who had notified us. This was only a stopgap and we knew a more manageable solution was required,” says Zak Harding, Touchpaper’s IT Manager.

Furthermore, spam was beginning to impact Touchpaper’s level of customer service. Support teams often need to send out visual basic script and executable files to customers experiencing problems with their Touchpaper systems. Unfortunately, the existing anti-spam software would wrongly prevent some of these emails from being sent, causing delays in issue resolution.

THE IRONPORT SOLUTION

Early in 2005, Touchpaper approached two security consultancies for recommendations on the best appliances on the market. The IronPort C10™ was recommended by both. As a result, Touchpaper decided to evaluate the technology (alongside an appliance from a competitor). The evaluation quickly proved that IronPort® was the best solution for Touchpaper’s requirements.

A challenge faced by many organisations today is managing the impact of large attachments on email performance and storage requirements. One of the benefits of the IronPort solution is its ability to manage the size of attachments by departmental needs. “For example, some departments – like marketing and sales – need to send and receive large files, such as PDF images, but most departments do not,” explains Harding.



Now that we have IronPort in place, IT resources are not drained from responding to employees email release requests. ”

— Zak Harding
IT Manager, Touchpaper



Touchpaper uses IronPort's Active Directory Integration to manage groups of users and assign appropriate privileges, such as attachment size, to certain teams or individual users. "Responding to email release requests from employees was the single biggest drain on IT resources," continues Harding. "The time we have saved is the main benefit to my team. Now we have IronPort in place such requests are rare."

Harding sums up, "Email management and security should be automated, reliable and (most importantly for both internal and external users) invisible. They just want to know that it works and, thanks to IronPort, it does."

Before the IronPort appliance went live, Touchpaper was receiving and quarantining 1,000 emails a day. Many of these messages were wrongly being blocked, but the vast majority were spam. Now that the new solution is in place, spam is a thing of the past.

**IronPort Systems, Inc.**

950 Elm Avenue, San Bruno, California 94066

TEL 650.989.6500 FAX 650.989.6543

EMAIL info@ironport.com WEB www.ironport.com

IronPort Systems, a Cisco business unit, is a leading provider of anti-spam, anti-virus and anti-spyware appliances for organizations ranging from small businesses to the Global 2000. IronPort appliances utilize SenderBase, the world's largest email and Web threat detection network and database. IronPort products are innovative and easy-to-use—providing breakthrough performance and playing a mission-critical role in a company's network infrastructure.

Copyright © 2000-2007 Cisco Systems, Inc. All rights reserved. IronPort, the IronPort logo and SenderBase are registered trademarks of Cisco Systems, Inc. All other trademarks are the property of Cisco Systems, Inc. or their respective owners. While every effort is made to ensure the information given is accurate, Cisco does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may be subject to change without notice. P/N 451-0119-1 10/07

IronPort is now
part of Cisco.

