

Case Study



**The Ohio Heart
& Vascular Center**

**Unclogging the Email System
for Better Health Care**

OVERVIEW

The Ohio Heart and Vascular Center has a culture of collaboration and early adoption of advanced technology. Working together with local hospitals and health care systems, the company strives to provide the most advanced care in the most convenient, accessible and seamless way possible.

Ohio Heart was founded in 1995, through the merger of five of the highest quality cardiovascular practices in the Greater Cincinnati area. As Ohio's largest cardiology group, it has nearly 250 employees in 12 locations. The company was the first in Ohio to use Tissue Plasminogen Activator (tPA) to dissolve a blood clot causing a heart attack, first in the country to use branch vessel stents and the first in the world to use a bipolar left ventricular pacing lead with guide wire delivery.



IronPort has one of the few products that simply works – they built a great solution that really solves the problems of email security management in my network. ”

OHIO HEART AT A GLANCE

Headquarters: Cincinnati, Ohio
 Locations: 12 regional offices
 Services: Advanced cardiology and healthcare
 Employees: 248
 Email System: Microsoft Exchange 2000

THE IRONPORT ADVANTAGE

- Major improvement in end-user productivity
- 100 percent improvement in filter effectiveness over previous system
- Reduced email administration time by 90 percent
- Reduced spam traffic to Microsoft Exchange server
- Reduced administrator time devoted to email system by 90 percent



THE SITUATION

Ohio Heart receives 42,000 inbound messages per day – only about seven percent of which are legitimate. The remainder of the messages are spam, or the result of viruses, directory harvest attacks and phishing attacks.

The company's older anti-spam appliance was unable to filter accurately, which resulted in an enormous database of quarantined mail that users had to check by hand. The system required frequent manual intervention, and active management of white- and blacklists.

“Our old solution simply did not perform well,” says Bill Hahn, Chief Information Officer at Ohio Heart and Vascular Center, Inc. “As we started looking for a new solution, we had four major concerns: the loss of end-user productivity, the burden on our IT staff to manage the old system, the need for easy message tracking and the ability to protect our Microsoft Exchange server.”

TECHNICAL CHALLENGES

Like other healthcare organizations, Ohio Heart is legally obligated to carefully manage its email system. Employees share a single Microsoft Exchange 2000 server, accessed primarily in office locations, but occasionally remotely, or via the Web.

In selecting a new email security appliance, the company had a number of concerns. The first was ease of integration with existing infrastructure, and with user habits. The new system couldn't change the way users read, wrote, or sent mail – but it had to greatly reduce the amount of spam, and the number of viruses that made it to users' desktops. That meant increasing the accuracy of the filtering, without creating false positives. In addition, the system had to reduce the amount of work done by the IT staff – in terms of both system maintenance and answering inbound help desk calls. Finally, the system was expected to generate positive user feedback, not simply an absence of complaints.

“Working with Data Processing Sciences (DPS), our trusted solutions provider, we reviewed the myriad of products in this space,” Hahn says. “Dan Baker, our DPS account representative, provided technical white papers, customer testimonials and ROI information – which we used to develop our evaluation criteria.”



We no longer quarantine suspect spam because, with IronPort, false positives have been eliminated. ”

– Bill Hahn, Chief Information Officer
Ohio Heart and Vascular Center, Inc.



THE IRONPORT ADVANTAGE

After an installation process that took less than one hour, the IronPort C10™ email security appliance eliminated a remarkable amount of spam at Ohio Heart.

“The IronPort® appliance blocks 90-95 percent of inbound spam, and that was something our users noticed right away. People used to complain to us about spam, and that just stopped as soon as we installed the IronPort appliance,” Hahn says. “We no longer quarantine suspect spam because, with IronPort, false positives have been eliminated.”

The IronPort C10 has also reduced the load on IT staff. Time spent managing the mail system has been dramatically reduced – from two to four hours per day to one to two hours per week. “Based on estimates of lost of productivity and IT management time, we calculated that we got a full return on our investment in just three months,” Hahn says.

Moving forward, Hahn says the company is planning to adopt IronPort Virus Outbreak Filters™, which detect outbreaks in real time – hours before signatures used by reactive anti-virus solutions are updated. Hahn is also looking at using the IronPort appliance to help enforce policies related to HIPAA, including outbound content filtering and encryption.

Hahn concludes, “IronPort has one of the few products that simply works – they built a great solution that really solves the problems of email security management in my network.”



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 451-0113-1 10/07

IronPort is now
part of Cisco.

