CUSTOMER

Case Study

IRONPORT®

JOHNS HOPKINS UNIVERSITY

Serving Up Healthy, Spam-free Email at One of the Nation's Top Universities

THE SITUATION

Founded in 1876, the Johns Hopkins University was the first research university in the United States. Today, it has a presence in China, Italy and Singapore, as well as many other countries, making it a world leader in teaching, patient care and scientific discovery, particularly in medicine. The School of Medicine opened in 1893, and was the first to integrate medical research, teaching, and patient care, as well as the first to admit women on equal terms with men.

> "We were up and running in a day with the IronPort appliances. End-user complaints about spam have dropped significantly, and we've been able to offload a large amount of burden from the internal mail servers."

JOHNS HOPKINS UNIVERSITY AT A GLANCE

Assets: First research university in the U.S.
Headquarters: Baltimore, Maryland
Locations: Multiple in-state and international campuses
Email: Multiple email systems with over 36,000 users
Challenge: Before installing four IronPort C60s, spam was more than 60% of total message volume

THE IRONPORT ADVANTAGE

- Protection for hundreds of on-campus mail servers
- Effective in heterogeneous environment; compatible with many mail systems
- Appliance functionality reduces staff costs
- SMTP Authorization supports university personnel while they travel
- LDAP routing per domain
- TLS support for improved security

THE SITUATION (CONTINUED)

Like other academic computing environments, Johns Hopkins has a decentralized approach to IT, a demanding user base, and more than a few users who are "curious" about its systems. With literally hundreds of mail servers installed in dozens of departments serving more than 36,000 users, protecting and managing the email system was a challenging but strategic project.

By late 2004, more than 60 percent of Johns Hopkins inbound email was spam, and the University was tasked with complying with regulatory requirements, principally the Health Insurance Portability and Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act (FERPA).

By working with IronPort®, the Messaging Team at Hopkins was able to resolve users' security issues, while ensuring regulatory compliance.

TECHNICAL CHALLENGES

"Meeting the needs of a diverse user population while adapting to the different Notes, Exchange, Groupwise, Irix, Solaris and other Unix-based systems was the first requirement for any solution," says Anthony Snead, a Senior Systems Software Engineer with the Enterprise Messaging Team of the Johns Hopkins Information Technology Service.

Another challenge was posed by an early anti-spam product, which was capable of blocking only 60 to 65 percent of inbound spam, and worse, created many false positives – preventing many legitimate messages from reaching their destinations.

The third challenge Johns Hopkins encountered was related to regulation. For a university conducting medical research and providing medical services, there are complex, HIPAA related regulatory requirements that revolve around email traffic. LDAP routing on a domain basis was needed to support the implementation of special email policies within certain domains. Transport Layer Security (TLS) was also required, particularly for email containing protected health information (PHI).

Finally, there was a need for secure off-campus access to the email system. Many of the University's faculty and staff travel worldwide and require remote access, so it was critical to provide the ability to send outbound email with SMTP authentication.

As the messaging team began their evaluation phase, they were able to quickly determine that they had two options: to custom configure software packages and hardware from different vendors, or to buy a multi-function, multi-vendor security appliance.

"We opted for a multi-function appliance to better ease deployment and maintenance. In addition, our staff can easily manage the system with minimal training," Snead explains. "Reviewing all of the products in our test environment allowed us to ensure we purchased the right solution. We simply needed something that would work, without constant care, or pagers going off at all hours of the night."

THE IRONPORT SOLUTION

With four IronPort C60™ email security appliances, two on each primary campus, the Johns Hopkins network perimeter is well protected. Inbound spam reaching internal servers has been reduced by more than 95 percent, and false positives have dropped to zero.

Used by eight of the top ten ISPs, IronPort C60 email security appliances combine market leading, best-of-breed anti-spam, anti-virus, encryption, digital rights management, and archiving technologies. These appliances run on IronPort's revolutionary MTA platform, providing the highest levels of email protection, with exclusive preventive and reactive technologies, and industry-leading email management tools.

With IronPort's management reporting features, the messaging team also has more information about how mail flows than ever before. "With our previous solution, we couldn't visualize what was going on with our systems," Snead recalls. The IronPort appliances allow us to see what is really coming into our network."

The IronPort C-Series™ email security appliances have also prevented late night service calls, and the compromise of on-campus machines – a few of which had been hijacked by spammers at various times.

"We were up and running in a day with the IronPort appliances," Snead says. "End-user complaints about spam have dropped significantly, and we've been able to offload a large amount of burden from the internal mail servers."

IRONPORT 02/05 DOC RELEASE

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.

IronPort is now part of Cisco.