CUSTOMER

Case Study

IronPort Provides Lessons in Email Security

OVERVIEW

With 29 elementary, 9 junior high and 5 high schools, as well as nearly 5000 staff, and 28,000 students, Weber School District is one of the largest K-12 school districts in Utah. The district is also a national leader in the use of instructional technology. All full-time and most part-time employees have desktop computers that are replaced every four years, and the district has installed broadband connections into nearly every classroom.

In addition to staff, more than 20,000 students are using webmail. The Weber School District technical team must protect them all from being exposed to inappropriate email – not only because that is district policy, but because the Childhood Internet Protection Act statement (required by federal programs) demands it.

> “We really like the hands off administration, which has helped decrease the time we spend managing the system, and reduced our overall security-related costs by about 20 percent.”

WEBER SCHOOL DISTRICT AT A GLANCE

Headquarters: Ogden, Utah
Locations: 34 K-12 schools and 6 offices
Services: Education for over 36,000 students
Employees: 5,000
Email System: Groupwise 7.1

THE IRONPORT ADVANTAGE

- Improved capture rate, with no false positives
- Prompt and reliable support
- Stability ensures zero downtime
- Increased filter effectiveness and manageability over previous system
- Reduced costs associated with lower loads on mail servers

THE SITUATION

Over 540,000 emails per day are directed to the students and staff of Weber School District, and more than 97 percent of those messages are spam. Not only is the content of these messages damaging to students, it can act as a vector for destructive desktop viruses, and overload the District's four Groupwise 7.1 servers.

Prior to working with IronPort®, Weber School District had a long experience with anti-spam appliances. However, previous solutions suffered from a low capture rate, false positives, occasional crashes (resulting in long periods of downtime) and unmanageable content filtering. These legacy systems also required frequent manual updates.

TECHNICAL CHALLENGES

As it began to look at replacing its email security solution, Weber School District had a number of requirements, including zero false positives, reliable content filtering, and stability and uptime, explains systems engineer, Alex Korkishko.

The new system couldn't affect how students and staff read, wrote or sent mail – but it had to substantially decrease spam, and the number of viruses that made it to users' desktops. That meant increasing the accuracy of the filtering without generating false positives.

As Korkishko began to evaluate alternative solutions, additional criteria were added to the list. "We really needed a high catch-rate and prompt, reliable support from the vendor," he says.

Virus scanning, protection from image-based spam, and support for outbound SMTP were other needs. Due to expense, and the lack of control, the option of using an anti-spam service was eliminated.

THE IRONPORT ADVANTAGE

In late 2005, Weber School District installed an IronPort C30™ email security appliance. The installation took less than six hours and the results were almost immediate.

"The spam catch-rate improved, without generating additional false positives," Korkishko says. "We really like the hands off administration, which has helped decrease the time we spend managing the system, and reduced our overall security-related costs by about 20 percent."

> “IronPort has delivered on every point promised to me. False positives have been dramatically decreased, the hardware appliance has been very stable, and hands on administration is now minimal.”

THE IRONPORT ADVANTAGE

“We are currently running both Symantec Brightmail and IronPort Anti-Spam™,” Korkishko says. “Since we switched to IronPort, we haven’t had any false positives.”

Weber School District is also running IronPort Virus Outbreak Filters™, which quarantine suspected viruses before signature files are available from traditional anti-virus vendors. “I see about two to three outbreaks per day, so I think it’s well worth the extra license cost.”

“IronPort has delivered on every point promised to me,” Korkishko concludes. “False positives have been dramatically decreased, the hardware appliance has been very stable, and hands on administration is now minimal.”

IRONPORT
02/07
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.

P/N 451-0106-1 10/07

IronPort is now part of Cisco.