CUSTOMER

Case Study

IRONPORT®

jetBlue AIRWAYS®

Leading Airline Soars with IronPort's Email Security Appliances

THE SITUATION

JetBlue Airways Corporation has prospered in the competitive airline industry by providing low-cost travel options for value-conscious fliers to destinations throughout the United States, the Bahamas, the Dominican Republic and Puerto Rico. By capitalizing on the efficiencies of electronic ticketing, and operating out of less crowded airports near major cities, JetBlue has emerged as one of the nation's leading value carriers. Its continued growth demands a state-of-the-art email network, based on a robust platform that delivers virus and spam prevention, while protecting the reputation of its outgoing traffic for delivery of critical customer communications (including itinerary confirmations and opt in promotion notifications).

> "IronPort Virus Outbreak Filters is a big winner for us. We now know that our network is protected, even as we wait for anti-virus signature updates."

JETBLUE AIRWAYS AT A GLANCE

Headquarters: New York, New York
Business: Low cost air travel serving 30 US markets, the Bahamas, the Dominican Republic and Puerto Rico
Industry Rank: Among nation's top ten carriers

THE IRONPORT ADVANTAGE

- Powerful, first line of defense for Microsoft Exchange servers
- Spam and virus filtering for threat protection at network perimeter
- LDAP recipient validation at the gateway
- Multi-layer, multi-vendor platform for inbound and outbound traffic
- Hassle-free manageability

DISCLAIMER: This document was originally published 02/05. While every effort is made to ensure the information included is accurate, Cisco does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may change without notice.

TECHNICAL CHALLENGES

JetBlue found its previous security system increasingly inadequate in its ability to block spam and viruses without creating troublesome false positives. The airline also required a solution that would save on administrative time and hassles. “We wanted a solution that could catch viruses and spam, and provide us with the ability to easily manage different servers from one central point,” said Hayk Chorekchyan, JetBlue’s Exchange Manager. After evaluating modifications to its existing security system, as well as offerings from three other vendors, the company found what it needed in the IronPort C-Series™ email security appliance . “Among the three systems we tested, the IronPort C60™ was the *only* solution which met all of our needs and required very little administrative intervention,” Chorekchyan explained.

THE IRONPORT ADVANTAGE

IronPort® provided JetBlue Airways with a multi-vendor, multi-layer email security solution that incorporates the industry’s best solutions from the market’s leading vendors of anti-spam, anti-virus, encryption, digital rights management and archiving technologies. Built from the ground up on IronPort’s high-performance MTA platform, the IronPort C60 provides cutting-edge security against virus outbreaks, spam attacks, phishing, false positives and content filtering for policy enforcement. The all-inclusive system provides fingertip control for JetBlue’s IT managers with centralized management that enables its administrators to manage multiple appliances without having to integrate additional hardware.

Advanced Virus Detection

Utilizing data from IronPort’s SenderBase® (a leading network of contributed data from over 100,000 organizations) IronPort Virus Outbreak Filters™ identify virus threats in real-time at their initial outbreak and quarantine them for scanning, typically several hours before anti-virus signatures are made available. In May of 2005, for example, IronPort Virus Outbreak Filters successfully thwarted the spread of the latest Sober virus variation, which infected 3.5 percent of all global email traffic. Less than two hours after its outbreak, the filters quarantined infected messages across the JetBlue network, before the first anti-virus signature was released.

The Industry’s Leading Reactive Filters

In addition to Sophos virus scanning, the IronPort C60 provides JetBlue with the best-in-breed spam detection from Symantec Brightmail. This delivers the industry’s most effective spam detection without incurring troublesome false positives. The IronPort C60 offers further threat protection by providing LDAP recipient verification at the gateway, immediately bouncing messages not bound for valid recipients within JetBlue’s active directories.

IRONPORT
02/05
DOC RELEASE

IRONPORT®

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.

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 451-0117-1 10/07

IronPort is now part of Cisco.

CISCO