

## Cox Communications

### Customer profile

Third-largest cable provider in the United States

### Industry

Broadband Communications

### IT environment

More than 50,000 corporate email addresses under the company's internal domain

### Challenges

Circumvent the need for additional Exchange servers due to exponential increase in spam volume; maintain zero false-positives and sustain success in blocking spam

### McAfee solution

McAfee Email Gateway (formerly IronMail) Appliance with Connection Control

### Results

- Generates zero false-positives
- Rejects 90,000 connections from obvious spam-sending sources each hour
- Reduces total email volume by 40%
- Eliminates the need for additional Exchange servers or McAfee Email Gateway appliances
- Slows spammer's bandwidth capabilities

## Cox Communications Stops More Than 90,000 Messages Each Hour with Connection Control of McAfee Email Gateway

Cox Communications is the third-largest cable provider in the United States, offering an array of services ranging from cable television, local and long distance telephone services, high-speed Internet, and commercial voice and data services. With more than 6.6 million total customers and 30,000 employees, Cox Communications is routinely recognized for its high capacity, reliable broadband delivery network, as well as its ability to provide best-quality customer service. In addition, local cable advertising, promotional opportunities and production services are sold under the Cox Media Brand. Cox Communications is also an investor in programming networks including Discovery Channel.

### Business Challenge

Cox Communications has more than 50,000 corporate e-mail addresses under its internal cox.com domain, and e-mail is a business-critical communication tool. Employees use e-mail to communicate with not only one another, but also with customers about services, upgrades and even billing information.

"As a multi-serviced communications company, which includes providing broadband Internet service, there are many instances in which people will confuse cox.com, our internal domain name, with cox.net, our ISP domain name," says Franklin Warlick, Messaging Systems Administrator for Cox Communications. "Because of this common mistake, we receive a large amount of e-mail, both legitimate and unwanted. It is critical for us to stop the spam messages from reaching our users, as some may contain system-damaging viruses, and all unwanted messages cost the company both time and resources."

Cox Communications decided to deploy McAfee Email Gateway (formerly IronMail) Appliance from McAfee's Network Security Business Unit (formerly Secure Computing). Cox Communications selected the product in 2004 because it was one of the early leaders in email security and they evaluated spam messages as a global threat. Additionally, with the increasing sophistication of spam, unsolicited messages can contain viruses and worms, as well as harmful phishing attacks. After deploying McAfee Email Gateway, Cox Communications found that less than four percent of the company's e-mail traffic was legitimate. But as spammers began to steadily increase the volume of messages, Cox Communications was faced with the dismal prospect of not only increasing the number of McAfee Email Gateway appliances, but also adding more Exchange servers in order to keep up with the continually increasing mail flow.

"In 2001 we were at 40,000 mail messages per month. In October 2004 that monthly number had risen to 40 million messages," says Warlick. "Although McAfee Email Gateway was blocking 30 million of those messages as spam and doing a great job protecting us at the edge without letting the bad stuff into the network, we were in desperate need of a solution to the mail volume issue.

Whether it required more McAfee Email Gateway appliances or Exchange servers, Cox was faced with a complicated and costly upgrade to our mail architecture—and it was all because of spam.”

### Selecting Connection Control

When Cox Communications initially evaluated McAfee Email Gateway in early 2004, the company was impressed with the product’s aggressive approach to spam blocking. This approach is driven by Spam Profiler, which analyzes over 1,000 user-definable characteristics of a message, weighs each of those characteristics and makes a decision on whether the message is spam or not. Just 10 months after deploying McAfee Email Gateway, Cox Communications’ mail volume had become practically unmanageable, and the increasing volume of spam was solely responsible. Rather than deploy additional McAfee Email Gateway appliances to handle the load, McAfee’s Network Security Business Unit approached Cox with a solution that would cost the company nothing: Connection Control.

Connection Control is the industry’s first offering to combine two innovative techniques: traffic shaping and reputation services. This combination dramatically increases the message handling capability of McAfee Email Gateway and reduces the cost for organizations to stop spam. Connection Control uses scores from McAfee Email Gateway’s unique Message Profiler technology to create a global reputation database of senders to identify obvious spammers, and then dynamically limits or rejects connections from offending senders.

### Immediate reduction in spam volume

After activating Connection Control, Cox Communications blocked nearly 4,000 individual Internet Protocol addresses the first night, and eliminated 90,000 unwanted messages immediately. McAfee Email Gateway’s Connection Control enabled Cox Communications to focus on the worst offenders and reject their spamming attempts at the edge. Furthermore, Cox’s total incoming spam volume dropped by approximately 40 percent within a few hours of turning on Connection Control.

“Without having deployed Connection Control to stop the most egregious spammers from even sending messages into the McAfee Email Gateway appliance, we would have ended up having to double the amount of appliances we currently have,” says Warlick. “Since upgrading our boxes to Connection Control the return on investment that we have experienced is significant. We have been able to process more mail with no incremental cost. In fact, we can even take one or two of our boxes offline to do maintenance without bringing traffic to a halt.”

In addition, maintaining zero false-positives is a very important factor for Cox Communications. Since upgrading with Connection Control, the company has continued to generate no false-positives. “As our mail rate has grown, we have been able to keep a lot of people out. It is also nice that Connection Control replies to spammers on an SMTP level, which requires some bandwidth on their end, dishing out a little bit of payback,” concludes Warlick.

---

*Since upgrading our boxes to Connection Control, the return on investment that we have experienced is significant. We have been able to process more mail with no incremental cost. In fact, we can even take one or two of our boxes offline to do maintenance without bringing traffic to a halt.*

Franklin Warlick  
Messaging Systems Administrator  
Cox Communications

---

