

Arlington County Government

Blocking Spam and Malware While Saving \$750,000 a Year
with Symantec Security Solutions

Inundated by spam and other network security problems, the Arlington County government struck back with a multi-layered defense using Symantec products. Symantec™ Mail Security appliances block spam at the gateway, reducing burden on email servers, and at the network level as well. At the client level, Symantec AntiVirus™ and Symantec™ Client Security provide protection against malware for the county's 3,800 users. The result is \$750,000 in annual savings in staff time, as well as 80 percent fewer messages in the county's email servers.

Organization Profile

The government of Arlington County, Virginia (www.co.arlington.va.us) has within its jurisdiction national strategic assets such as the Pentagon, Ronald Reagan Washington National Airport, and 40 other federal agencies.

Industry

Government

Solution

Information Security

Dispatches from the front

The war on spam is intensifying. The government of Arlington County, Virginia (Arlington) has made the following observations about recent trends in spam:

“Before we got the Symantec Mail Security appliances, there were some conservative estimates that spam cost Arlington County \$750,000 a year.”³

The source of spam is more concentrated than one might think. In one week just four IP addresses, discovered to be primary sources of spam, made over one million requests to the Arlington County network to connect. Those requests were denied.

Incoming waves of spam are focused on specific times of the week. Most of the day's spam arrives just after midnight. Most of the weekend email is spam.

The IP paths of incoming spam messages are disguised. Arlington's incoming email seemingly arrives via 250,000 different IP paths each week. But nearly 70 percent of these paths carry between 91 and 100 percent spam. Legitimate email tends to use just three percent of incoming paths, which carry 90 to 100 percent genuine email.

More than a nuisance – a threat

Up until mid-2005, Arlington's email servers were being flooded with 80 percent spam—100,000 unwanted email messages per day—and the percentage was growing.

David Jordan

Chief Information Security
Officer
Arlington County
Government

Symantec Mail Security appliances block spam to reduce incoming email from 125,000 to 25,000 messages a day.

This is more than an inconvenience. Arlington County measures just 26 square miles and is one of the smallest counties in the nation in terms of land area. Nevertheless, it is one of the nation's most strategic counties. Its border is just two miles from the White House, and within its boundaries lie the Pentagon, Ronald Reagan Washington National Airport, and 40 other federal agencies. Arlington County's police, medical, and fire departments are first responders to emergencies at these locations, and the county's computer network helps coordinate them.

network stays secure, efficient, and available. Jordan is no newcomer to policing malicious behavior in the high tech arena. He came from MCI, where he founded and directed the technical security team, which was dedicated to stopping phone hackers from stealing telecommunications services.

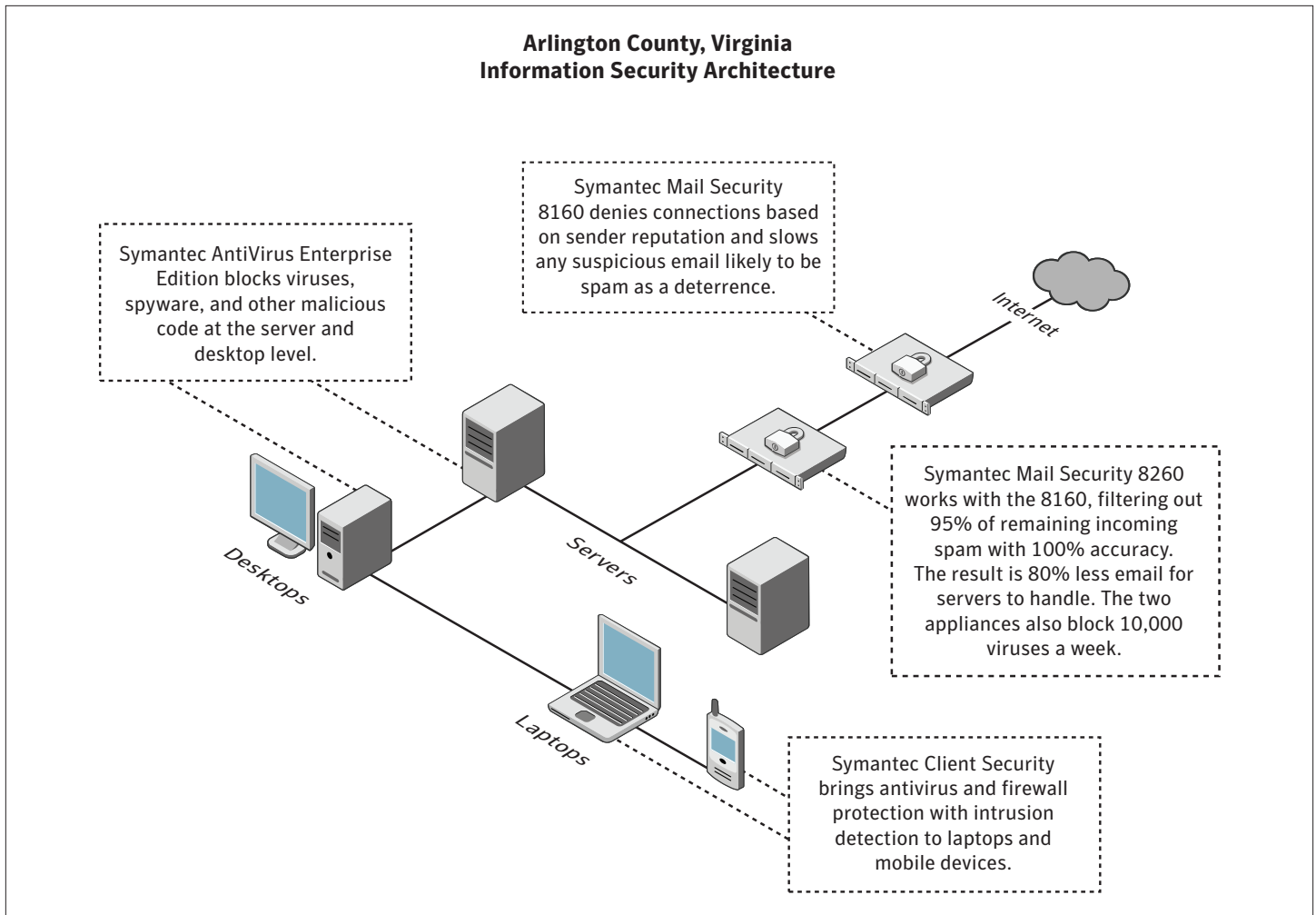
When he joined the Arlington County government, antivirus security was not adequate, he recalls. "About once a month, one of the tech staff would send a mass voicemail to the workforce regarding the latest virus and how to deal with it."

Assigning a team

Five years ago, Arlington County brought in Chief Information Security Officer David Jordan and a team of other IT specialists to make sure its

Symantec to the front lines

"Almost immediately, we brought in Symantec AntiVirus," Jordan continues, "and we've grown up together." Arlington County chose



Symantec because of its strong reputation, which was validated by experience. “The first thing we noticed about Symantec is its people,” Jordan recalls. “They’re high-quality, well-skilled, and love what they’re doing. The second is process: the way Symantec articulates security issues, the quality of its manuals, its Web site, the speed of its response. And there’s its technology: we looked at the acquisitions Symantec has made over the last five years. They are well thought-out with the big picture—the long view—in mind. That’s the kind of people you want to surround yourself with in solving problems: winners and thought leaders. Symantec is the beacon of leadership in that regard.”

“We got the Symantec Platinum Protection plan,” Jordan continues, “so we could get a good handhold when we needed one as we learned virus security. We developed policies to push out definitions in a timely manner. It wasn’t until we started making the place secure that additional money for security became available. People weren’t getting the mass voicemails about viruses anymore. Their machines weren’t crashing. The infection rate dropped to the point where today it’s in the background.”

More recently, Arlington began to upgrade to Symantec™ Client Security software on its servers and workstations. This product combines Symantec’s well-known antivirus protection with firewall and intrusion protection, providing comprehensive and proactive protection against blended threats, spyware, unauthorized network access, and mass-mailer attacks, with virus and vulnerability-based detection.

Strengthening defenses

With the virus problem arrested, Jordan’s team focused on stopping spam, and employed a number of tactics. “Among the members of the IT team, we were spending 600 hours a

SOLUTION AT A GLANCE

Business Drivers

- Protect the computer network serving first responders to crucial national facilities
- Maximize county government productivity and security through email
- Minimize productivity loss due to spam and security threats

Technology Drivers

- Block malicious code from disrupting network
- Block spam while eliminating false positives
- Provide protection to mobile workers while outside network defenses

Solution

- Comprehensive email and client security solution from Symantec

Symantec Products

- Symantec™ Mail Security 8260
- Symantec™ Mail Security 8160
- Symantec AntiVirus™ Enterprise Edition
- Symantec™ Client Security

Technology Environment

- Applications: Police and Fire Records Management, Online Bill Payment, Emergency Text Alert System, Online Permits
- Databases: Personal Property Tax, GIS, Building Permit database, Employee Payroll, Electronic Records Management (Arlington PRISM)
- Server platform: Dell 6650 servers running Windows 2003 and Linux
- Workstations: Dell GX620

Symantec Services

- Symantec Platinum Support

year battling the spam problem with different solutions, most of them home-grown,” says Chris Hartley, one of the lead engineers in the Arlington’s network engineering group. “That doesn’t count the time that our 3,800 employees were spending deleting spam.”

Jordan’s team decided to center on one industry solution, and in a review decided that Brightmail AntiSpam technology was the best choice because of its focus on sender reputation. Jordan sent a suggestion to Symantec that the technology be acquired. A few months later, Symantec acquired it. Obviously,

“Thanks to Symantec, viruses are not an issue for us, and now with the Symantec Mail Security 8160 and 8260, neither is spam. We went from 125,000 messages a day to 25,000, an 80 percent reduction.”

David Jordan
Chief Information Security Officer
Arlington County Government

BUSINESS VALUE AND TECHNICAL BENEFITS

Cost Savings

- \$750,000 in staff time saved annually by blocking spam
- \$280,000 average cost per virus incident prevented (2002 FBI Crime and Security Survey)

Return on Investment

- 100% payback in one year for Symantec Mail Security devices

Enhanced Security

- 80% reduction in email processing, from 125,000 messages a day to 25,000, by blocking spam
- Over 10,000 viruses detected and blocked at gateway each week
- Over 500,000 connections by spammers denied each week

“Spam is greatly reduced, and we experienced only one false positive per 2 million emails while fine tuning the application, and have not experienced a single false positive since. We are not blocking any legitimate mail. That’s the bottom line.”

David Jordan

Chief Information Security Officer
Arlington County Government

Jordan was not the only one who saw the match between Brightmail and Symantec technology.

“We were thrilled to see Symantec make Brightmail technology available in a mail appliance,” Jordan says. In mid-2005, the county evaluated the products and decided to purchase two appliances from Symantec to form a multilayered antispam defense strategy.

Stopped at the gate

Located on the perimeter, the Symantec Mail Security 8160 appliance is a bandwidth-limiting tool. It evaluates the type of email coming down any path and establishes a reputation for that path. Then it uses patent-pending traffic shaping technology to deny or approve connections based on sender reputation, reducing the volume of spam before the spam ever hits mail servers.

During the initial few weeks of operation, Arlington County’s Symantec Mail Security 8160 appliance denied over a million connections from paths that

have a reputation for sending spam. Should any other paths begin to look suspicious, the solution slows down the emails they carry, sending back messages that delivery will be delayed. “It ties up spammer resources at no cost to us and makes our servers unattractive to spammers,” Hartley says. “Legitimate email gets through, but spammers get paid by the volume of spam they deliver, so they’re motivated to move on to more profitable targets.”

Multiple filtering defenses

Inside the perimeter, as a second layer of defense, the Symantec Mail Security 8260 employs Symantec Brightmail AntiSpam technology to filter out spam, viruses, and unauthorized content. Brightmail uses 20 filtering technologies to block 95 percent of spam¹ with an industry leading accuracy rate of one false positive in one million emails.² It receives updates on known spam sources every five to ten minutes from a global Symantec probe network.

“Symantec has the largest sensor network in the world,” Jordan says. “Tying all those sensors together and

focusing them on the spam problem offers a huge benefit.” Adds Chris Hartley: “Spam is greatly reduced, and we experienced only one false positive per 2 million emails while fine tuning the applications, and have not experienced a single false positive since. We are not blocking any legitimate mail. That’s the bottom line.”

Improving email performance

David Jordan sums up the County’s gains. “Thanks to Symantec, viruses are not an issue for us, and now with the Symantec Mail Security 8160 and 8260, neither is spam. We went from 125,000 messages a day to 25,000, an 80 percent reduction. Our email servers can now do the job they’re designed to do.

“Before we got the Symantec Mail Security appliances, there were some conservative estimates that spam cost Arlington County \$750,000 a year³ in lost employee productivity, bandwidth costs, storage costs, and support costs. We now have those resources back for better uses.”

Stopping viruses

In addition, the Symantec Mail Security appliances are detecting and blocking over 10,000 viruses at the gateway each week. And at the server and desktop level, Symantec AntiVirus software is blocking viruses, spyware, and other malicious code. When key county employees take laptops and mobile devices outside the network, Symantec Client Security protects them by combining antivirus, a firewall, and intrusion detection on each device.

It's difficult to estimate the damage that a virus could cause Arlington County, but the average incident costs over \$280,000, according to the 2002 FBI Crime and Security Survey.

Fast payback and time for valuable projects

If the value of the protection, blocking, and freed resources is added up, according to Hartley, "we received 100 percent payback on the Symantec Mail Security appliances in one year."

Part of that payback is the 600 hours a year the IT team no longer spends fighting spam. It's time they can devote to more valuable projects

One is the county's new mobile command center, a vehicle enabling county government to continue essential business if its facilities are disrupted, or to coordinate government services at a large public event such as a marathon. Another is e-government, enabling citizens to conduct business with the county 24/7 online. And a third is the 24/7 wireless Internet access the county provides free of charge at public libraries and other hotspots.

"The constituents of Arlington County love these projects," Jordan and Hartley conclude. "If your enterprise is stable, if you aren't fighting viruses, and you aren't fighting security threats, this is the kind of value that an IT team likes to add."

1 eWeek 2003

2 Yankee Group Report 2004

3 Based on 3800 mailboxes (users) at an average loaded employee cost of \$35/hr and three seconds to delete each spam message