



## City Government of Buenos Aires

### Securing Vital Networks with Symantec Multi-tier Protection

**After a virus shut users out of the network for 12 hours, the Government of Buenos Aires knew it needed a better security solution. Symantec Multi-tier Protection met all of the city's requirements, providing single-console management, graphical reporting, spyware protection, and antivirus protection for Linux. The solution has greatly reduced downtime due to malware, improved efficiency with a single management console, reduced the spam that reaches users to almost zero, and saved more than 450 staff hours annually previously devoted to dealing with spam.**

#### ORGANIZATION PROFILE

With 200,000 employees, the City Government of Buenos Aires in Argentina ([www.buenosaires.gov.ar](http://www.buenosaires.gov.ar)) oversees nearly everything that happens in this cosmopolitan city of 12.4 million, from hospital and fire services to urban planning and the arts.

#### INDUSTRY

Government: State and Local

#### SOLUTION

Endpoint Security

#### The Challenge

Sometimes referred to as the “Paris of South America,” Buenos Aires has a rich heritage exemplified by classic European architecture, top-notch museums, a vibrant cultural scene, and world famous tango clubs. It is also the financial and commercial hub of Argentina and has one of the world’s busiest ports.

With 200,000 employees, the municipal government manages every aspect of life in the city, from hospitals and emergency response to education, urban planning, and the arts. Sustaining all this activity is the government’s computer network, serving 10,000 users and incorporating a wide range of applications, including the city’s 103 emergency response system (similar to 911 in the U.S.), budgeting, and administration among many others.

**“Symantec came closest to all our requirements.”**

**Gustavo Linares**

Chief Information Security  
Officer

Government of Buenos Aires

The network was protected with an antivirus solution from Trend Micro, but the government’s IT staff was increasingly dissatisfied with the product. For one thing, IT staff had to manage network security from several interfaces instead of one. Also, though the Trend Micro product provided virus protection, the government had to install a separate product to guard against spyware. Additionally, the Trend Micro product did not offer protection for the Linux-based computers in several departments.

Worst of all, Trend Micro’s Argentina operation could not seem to provide adequate support for the product. “It had problems, perhaps just like any product normally would,” says Gustavo Linares, chief information security officer for the Government of Buenos Aires. “Unfortunately, there just was not enough support to fix those problems when they came up.”

With its antivirus solution running at less than optimum, the city discovered—the hard way—that it was vulnerable to attack. “A virus corrupted the SQL database of registered users of our network,” Linares says. “All users were denied access to the system for about 12 hours.” It took 45 people, working for three or four days, to remediate the problem, he adds.

Symantec Mail Security for SMTP eliminated spam that got through the previous solution's filter.

**“More than 25 percent of the mail users received used to be spam, but that's been almost eliminated.”**

**Gustavo Linares**

Chief Information Security Officer  
Government of Buenos Aires

## The Solution

Convinced it was time for a new security solution, the IT staff evaluated four different security solutions in August 2007—from Trend Micro, Panda Security, McAfee, and Symantec. Although Symantec™ Multi-tier Protection was not the lowest cost option, “Symantec came closest to all our requirements,” Linares says. “And it came very close to our budget.”

Symantec Multi-tier Protection combines Symantec™ Endpoint Protection with malware protection for the heterogeneous environment of the typical enterprise. Symantec Endpoint Protection provides antivirus, antispymware, desktop firewall, intrusion prevention, and application and device control technologies, all controlled through a single agent.

Why was Symantec Multi-tier Protection the right choice? “There were legal compliance requirements that would only work with the Symantec product,” Linares says. “Also, it fit 100 percent with the technical requirements we had. And it uses fewer resources on the desktop, which is one of the aspects we value very highly.”

The single console in Symantec Endpoint Protection provides benefit as well. “That was one of the requirements in our technical specifications, and it was one of the problems we had with the Trend Micro solution—it had to be managed from different consoles,” Linares says.

In addition, he says, the Web-based graphical reporting provided by Symantec Endpoint Protection is a big help. “A network of thousands of people is not easy to control, so the reports are very important to us,” he says. “The fact that Symantec incorporates spyware and adware protection as well means we no longer need to use two different solutions. It's very important to us that this is now all in one product,” Linares says.

In addition, he appreciates the antivirus protection for Linux provided by Symantec Multi-tier Protection. “Various city offices are dependent on Linux, and before this acquisition, we had no antivirus protection for them,” he says.

## The Results

The city selected Symantec in October, and the solution was deployed in December. At the same time, the IT staff also implemented another component of Symantec Multi-tier protection—Symantec™ Mail Security for SMTP—to reduce the amount of spam coming into its network.

Even after just a couple of weeks of use, Mail Security for SMTP had already demonstrated its value. “More than 25 percent of the mail users received used to be spam, but that's been almost eliminated,” Linares says.

With the former Trend Micro solution, he says, 45 to 50 percent of incoming mail was filtered out as spam. With Symantec Mail Security for SMTP, that percentage has risen to 65 percent. In the old days, the spam the filter missed had to be dealt with by staff. “Now, it seems that almost no spam gets through,” he says.

The reduction in spam has resulted in a big time savings in staff time, he adds. With the previous solution, users not only had to spend time dealing with spam, they also sent spam reports to IT administrators. And two administrators had to spend an hour each per day, one in the morning and one in the afternoon, manually eliminating spam from users' mailboxes. In IT staff time alone, therefore, Mail Security for SMTP has produced a savings of more than 450 staff hours a year.

Symantec partner ComPlus Seguridad Informática helped the Government of Buenos Aires through product evaluation and implementation of the Symantec solutions. It also provides the first line of support for these products. “They are very helpful,” Linares says. In addition, the Government of Buenos Aires has Symantec Essential Support Services to provide 24-hour support for the products—another element that was required in the government's specifications.

Future plans include possible activation of the optional Network Access Control feature that is integrated into the Symantec Endpoint Protection agent. This would provide further protection to the city's network when employees such as inspectors reconnect

their laptops to the network after working away from the office. The government may also use Symantec Consulting Services on two important future projects: creation of a security policy manual and vulnerability testing to ensure that the network is fully protected.

When asked how long it may take for the Government of Buenos Aires to realize payback on its Symantec investment, Linares says, “This is a different evaluation for a government, when you consider the importance of the information. If there were an attack on government information, confidence in the government would drop immediately. There would be impact on the city—there would be quantitative damage. Therefore, payback for a product that protects the government network is considered to be immediate.”

This is why, he says, the relationship with Symantec is so important. “It’s very important for us to entrust our security to a company dedicated to security. Before this acquisition

## SOLUTION AT A GLANCE

### Key Challenges

- Prevent downtime and remediation costs due to malware incidents
- Improve local support for endpoint security infrastructure
- Provide security for Linux-based desktops and servers
- Simplify security management and reporting
- Consolidate antivirus and antispam solutions
- Achieve compliance with city regulations

### Solution

Streamlined and consolidated endpoint security solutions with single administrative console; strengthened network security; reduced spam

### Symantec Products

- Symantec™ Multi-tier Protection

### Symantec Services

- Symantec Essential Support Services

### Symantec Partner

ComPlus Seguridad Informática ([www.complus-arg.com.ar](http://www.complus-arg.com.ar))

### Technology Environment

- Applications: Numerous licensed and homegrown applications, including the Gobierno's 103 emergency system (similar to 911 in the U.S.) and the government's accounting and budgeting application
- Databases: SQL Server 2005, Oracle 7, MySQL 5, PostgreSQL 8.2
- Servers: About 80 servers, mostly HP and IBM, running Microsoft Windows Server 2000 and 2003, Sun Solaris 10, Debian 4.0, and Linux

### Business Results

- More robust protection against downtime and remediation costs of malware incidents
- Antivirus protection for Linux servers and workstations
- Projected IT staff time savings through single console management for endpoint security
- Consolidated virus and spyware protection
- Almost zero spam reaches users, down from more than 25% of incoming mail
- More than 450 staff hours per year saved eliminating spam [Buenos Aires, this is based on two staff members/one hour per day each, multiplied by about 48 weeks]
- Achieved compliance with city regulations
- Immediate full payback for Symantec Multi-tier Protection