

Comune di Milano



Hardening the Network and Streamlining Security Administration with Symantec Enables City to Expand Web-based Services

While expanding its network services, Comune di Milano was hit with a series of malicious code attacks. Turning to Symantec for comprehensive enterprise security solutions has enabled the city to end significant disruption from malicious code for all but the oldest systems, regain 41,000 hours in employee productivity lost to spam, and spot and repair compromised systems before their problems spread.

Challenge

The IT infrastructure of the city government of Milan is in the midst of transformation. So far, 200 of its 700 buildings—with over 10,000 PCs—have been connected with an optical fiber-based municipal area network (MAN) with new switches and other hardware. By 2008, the network will reach 700 buildings with dedicated gigabit Ethernet links. Systems on this network host many terabytes of sensitive data such as tax accounts, academic records, fines, parking tickets, and management tools for services such as water delivery and building permits.

Three main types of users need to connect externally to get the city's work done. Government employees connect from remote locations. Citizens need information on items such as permits, taxes, and fines. And over 800 contractors and consultants need access to do their work.

In 2001, the network was hit with several virus and worm attacks, such as Nimda. Thousands of systems were affected, and services slowed down or stopped for as long as two or three days at a time. Ever since, the IT team has been working to enhance network protection by consolidating, centralizing, and automating security processes.

Solution

After the 2001 attacks, the city asked for help from the antivirus vendor it had at the time, and from Symantec. "Symantec gave us the right help faster than the antivirus vendor we had before," says Enrico Fedeli, chief information security officer for Comune di Milano. "As a result, we replaced that vendor's solution with more than 10,000 seats of Symantec AntiVirus™ Enterprise Edition."

Meanwhile, the city was also increasing the variety of services offered over the Web. To protect Web servers against zero-day attacks, the IT team deployed Symantec Critical System Protection, which hardens the city's most important systems and helps maintain compliance by enforcing behavior-based security policies and enabling the operating system to be locked down.

ORGANIZATION PROFILE

With a population of 1.5 million, Milan (www.comune.milano.it) is the second largest city in Italy and a world center for design and fashion. The city government of Milan spans 700 buildings and has about 20,000 employees.

INDUSTRY

Government: Local

SOLUTION

Endpoint Security, Security Management, Messaging Security, IT Policy Compliance

“Symantec gave us the right help faster than the antivirus vendor we had before. As a result, we replaced that vendor’s solution with over 10,000 seats of Symantec AntiVirus Enterprise Edition.”

Enrico Fedeli,

Chief Information Security
Officer
Comune di Milano

Blocking spam is giving city employees more than 41,000 hours in added productivity each year.¹

The team also deployed Symantec Enterprise Security Manager™ to automate inspection of the servers for vulnerabilities and to ensure compliance with internal regulations.

Spam was becoming an acute problem and now makes up 90 percent of incoming messages. To block spam, the city deployed Symantec Brightmail AntiSpam™ software on servers and Symantec Mail Security 8260 appliances at the gateway.

For an added layer of protection with 24x7 monitoring of its firewalls and intrusion detection solutions, the city delegated surveillance in 2004 to Symantec Managed Security Services, and has counted on them ever since.

Comune di Milano receives licensing and other support from its team of Symantec partners, including KBE Srl, Nextiraone Srl, and Uniteam Srl.

Results

Since switching to Symantec AntiVirus Enterprise Edition in late 2001, the city has experienced no significant disruptions from malicious code, except a serious problem which involved the city's oldest Win 95/98/NT PCs.

Spam is also no longer a problem. "Thanks to the Symantec solutions, about 95 percent of spam is now blocked, and false positives are virtually non-existent," Fedeli says. "Our employees used to spend minutes every day looking for genuine messages and deleting spam. With 11,000 email accounts, we gain back thousands of hours in productivity and hundreds of gigabytes in email storage space by controlling spam."¹

The city's SMTP infrastructure is protected by three Symantec Mail Security 8260 appliances at the gateway. Besides blocking spam, the solution also scans every incoming and outgoing message to stop transmission of malicious code.

Network security has been strengthened since 2004 through 24x7 external monitoring by Symantec Managed Security Services. "People working in Symantec Managed Security Services Security Operations Centers, spread worldwide, have contacted us by phone several times when they spotted a compromised system on our wide network. Warnings are sent by mail at least every day. Besides an alert, they give us advice on how to fix the problem, so we can stop it before it can grow."

"This high level, 24-hour monitoring activity is almost impossible to deploy in-house," Fedeli adds. "Too many skilled people would be needed, much more than we can afford."

The IT team is evaluating Symantec Network Access Control, which ensures that endpoints are compliant with antivirus and other security policies before they're allowed to connect. They're expecting a great synergy together with 802.1x feature, available with new switches.

The team also expects to upgrade its Symantec AntiVirus solution to Symantec Endpoint Protection 11.0 in late 2007. Symantec Endpoint Protection offers the benefit of essential security technologies (antivirus, antispyware, desktop firewall, intrusion prevention, device control, and optional Network Access Control) via a single integrated agent and is administered from a single management console.

"Symantec Managed Security Services has contacted us several times when they spotted a compromised system on our network. Besides an alert, they give us advice on how to fix the problem, so we can stop it before it can grow."

Enrico Fedeli

Chief Information Security Officer
Comune di Milano

“Symantec Endpoint Protection has the kind of consolidated security I’m looking for to simplify management of our 10,000 PCs,” Fedeli says. “We want to combine it with Symantec Network Access Control. With secure endpoints, we can consolidate security with a single management console.”

The IT team is also evaluating Symantec Enterprise Vault to enhance archiving and eDiscovery of email and gain control over rapidly growing email storage.

Symantec Essential Support Services provides 24x7 assistance. “When I open a ticket with Symantec, I get good results,” Fedeli says. “Their network is extensive: The help we need is always available when we need it.. It’s better support than I’ve found from any other company.”

¹10,000 accounts * 1 minute saved/day = 10,000 minutes/day
= 166 hours/day*250 working days/year = 41,600 hours/year

SOLUTION AT A GLANCE

Key Challenges

- Expand services while enhancing protection of confidential citizen data
- Increase protection against malicious code and intrusions
- Gain increased control over endpoints, ensuring compliance
- Reduce productivity loss from spam
- Streamline system management

Solution

Endpoint, message, and infrastructure protection from a multilayered Symantec defense, and efficiencies from Symantec system management tools

Symantec Products

- Symantec AntiVirus™ Enterprise Edition
- Symantec Enterprise Security Manager™
- Symantec Critical System Protection
- Symantec Brightmail AntiSpam™
- Symantec Mail Security 8260
- Symantec™ Endpoint Protection (evaluation)
- Symantec™ Network Access Control (evaluation)

Symantec Global Services

- Symantec Managed Security Services
- Symantec Essential Support Services

Symantec Partners

- KBE Srl
- Nextiraone Srl
- Uniteam Srl

Business Results

- No significant disruption from malicious code since switching to Symantec (except those PC’s with an old, non-patchable operating system)
- 41,000 hours/year in productivity gained due to blocking 95 percent of spam with virtually no false positives¹
- Hundreds of incidents of compromised systems identified and repaired fast due to external monitoring
- Thousands of hours a year in travel time saved due to remote system deployment and management