



## Tribunal de Justiça do Espírito Santo

Protecting Vital Records as Brazilian Court System Goes Paperless with Symantec and ISH Solutions



**Vulnerable to attack, the network of the court system in the Brazilian state of Espírito Santo was down for as much as 20 days a year. Since deploying comprehensive security solutions from Symantec and its partner ISH, downtime from security incidents has been cut to zero. Almost all spam, as well as some 30,000 incoming viruses, worms, and Trojan horses a month are now being blocked or quarantined. As a result, security administration time has been reduced by 75 percent, and thousands of IT staff hours are now available for more valuable projects.**

### ORGANIZATION PROFILE

Tribunal de Justiça do Espírito Santo (TJES, [www.tjes.gov.br](http://www.tjes.gov.br)) is the court system for the state of Espírito Santo, located on the southeast coast of Brazil. Approximately 5,000 employees in 75 locations run a court system that serves the state's three million residents. At 17,800 km<sup>2</sup>, Espírito Santo is approximately twice the size of the U.S. state of Maryland.

### INDUSTRY

Government: State and Local

### SOLUTION

Endpoint Security, IT Policy Compliance, Data Protection, Client Management

### The Rule of Law

On the southeast coast of Brazil, just north of Rio de Janeiro, the state of Espírito Santo is home to three million residents. At 17,800 square kilometers, it's about twice the size of the U.S. state of Maryland, and includes within its borders beautiful beaches, lush rainforests, mountains higher than 2,750 meters (9,000 feet), and the biggest steel-producing city in the world: the state capital, Vitória.<sup>1</sup>

Administering justice in this state is a court system known as Tribunal de Justiça do Espírito Santo (TJES). TJES has 75 locations and 5,000 employees, and this wide distribution makes the computer network that connects it critical to effectiveness and productivity.

The IT team at TJES—and the IT team at every other law enforcement organization in Brazil—faces a particularly tough challenge: protecting against computer crime. Brazil has been characterized as being a major exporter of malicious code. People who break the law in Brazil not only have a motive to interfere with law enforcement computer networks, they also have world-class hacking expertise close at hand.

### Assault with malicious intent

Before 2005, the Tribunal de Justiça's IT network had a high vulnerability to attacks. The IT team believed that the network's intrusion protection was not adequate. They knew they needed to better protect the court system's confidential documents, and ensure they could be reviewed and altered only by authorized users.

Another security objective for the team was to strengthen defenses against viruses and malicious code. As many as 20 days a year of network operation were being lost to disruption from these threats.

**“Symantec and ISH actually exceeded our expectations by having a very fast response time and incredible reduction in downtime.”**

**Victor Murad Filho**

IT Director  
Tribunal de Justiça do  
Espírito Santo

Symantec Security Information Manager has reduced daily security monitoring from four hours to 15 minutes.

**“There was a lot of resistance to outsourcing because people want everything done internally. Now that everything is working and downtime has been drastically reduced, there is no more resistance. They are thinking about using outsourcing for other processes as well.”**

**Victor Murad Filho**

IT Director

Tribunal de Justiça do Espírito Santo

Spam was yet another problem, making up as much as 40 percent of each day’s email. As a result, TJES’s 4,000 email users needed to spend as much as 20 minutes a day sorting through inboxes and deleting spam. Occasionally, they overlooked or deleted legitimate email messages—a serious problem in a court system.

In general, it was difficult for the 25-person IT team at TJES to get the time needed to work on security issues because they also faced the task of caring for 4,000 computers. Just to provision or reversion one of these PCs took two to three hours, not counting travel time. This task needed to be minimized.

The need for security became much greater in 2007 when TJES moved to a paperless system, with all its processes digitized and stored on its servers. “This information is very, very confidential and has a high value,” says Victor Murad Filho, the court system’s IT director. “There may be judgments or suits that are worth millions and millions of dollars.”

### Learning to Love Outsourcing

TJES knew it needed outside help to secure its systems quickly. “We did not have the people on staff to do this at the speed we needed,” Murad Filho says. “Nobody was trained in security, or qualified to work on complex security solutions.” After carefully reviewing several different security solutions and partners, TJES selected Symantec as a vendor and Symantec Business Partner ISH Tecnologia Ltda. as its outsourcer.

At first, there was a lot of resistance outsourcing within TJES. Outsourcing was a relatively new concept in Brazilian governments at the time, and “people wanted to do everything internally,” he says. But ISH soon proved itself. For one thing, it only took half the time to get security solutions up and running that it would have with internal staff.

And it was hard to argue with the improvements. “In the past, sometimes things would go out for about 12 hours and we wouldn’t know whose responsibility it was to fix it,” Murad Filho says. “Now response times are sometimes as fast as 15 or 30 minutes.” This benefits not only the IT staff of TJES, but also the citizens who interact with the court. “Complaints can be processed and judged much faster, reducing stress and other problems. In the past, people had to wait a long time for a response or a judgment or ruling.”

Now, Murad Filho says, there is no more resistance to outsourcing—in fact, some other agencies have decided to give it a try. “Other local governments saw this as a great opportunity, so they have also started outsourcing some of their security services,” says Bernardo Santos Wernesback, consultant at ISH. “We even have governments in other states that have outsourced with us.”

### How to Make Protection Comprehensive

“The defenses we set up for TJES,” says Carlos Brandão, chief technology officer at ISH, “call on multiple layers of protection, for comprehensive security protection.” The IT team has been pleased with the result. “We lost as many as 20 days a year to security incidents before deploying Symantec solutions in early 2005,” says Murad Filho, “and zero days since.”

The outside layer of protection includes the Symantec™ Mail Security 8260 appliance. It calls on Symantec Brightmail™ AntiSpam technology to block spam with 95 percent accuracy and virtually no false positives. With spam blocked, the volume of incoming email at TJES has been reduced by up to 40 percent. Email servers are performing better, and court employees are more productive.

“Within 72 hours of deploying the Symantec Mail Security appliance, spam virtually stopped hitting our inboxes,” Murad Filho says. “Hundreds of users contacted our IT team to congratulate us and ask us what we had done. It was a miracle.”

Eliminating the five minutes a day employees spent deleting spam provides 8,000 hours a year in productivity gains at TJES.<sup>2</sup>

“Spam was also eating up disk space,” Murad Filho adds. “Since we blocked it, we need about 50 percent less disk space to store email.”

### Blocking More Than Spam

Reports from the Symantec Mail Security appliance show that since deployment in early 2005, it has blocked more than 5,000 incoming email-borne viruses, and about 100 viruses in outgoing email.

Another feature in the Symantec Mail Security appliance is its ability to conduct content filtering. TJES has set the appliance to detect confidential court documents and prevent them from being emailed in an unauthorized fashion. To support this, the IT team worked with security consultants from ISH to write 10 custom rules that the Symantec appliance enforces. “The content filtering capability in our Symantec solution brings much peace of mind,” Murad Filho says.

### Deeper Layers of Defense

Inside the TJES network are several additional layers of protection. Symantec AntiVirus™ Corporate Edition runs on servers to automatically detect and repair the effects of spyware, adware, viruses, and other malicious intrusions.

Symantec™ Client Security software runs on desktops and laptops, where it provides intrusion protection, antivirus, anti-spyware, and firewall capabilities. Having this endpoint security on laptops is especially valuable when users log onto the Internet from outside the firewall.

**“In the past, IT staff spent about 35 percent of their time fixing some kind of security problem, especially viruses and spam. Symantec solutions vastly reduced the time we spend fixing these problems.”**

**Victor Murad Filho**

IT Director

Tribunal de Justiça do Espírito Santo

## SOLUTION AT A GLANCE

### Business Drivers

- Enhance security against internal and external threats
- Maintain availability of data for court operations
- Boost productivity by minimizing spam
- Reduce the total cost of ownership for networking security
- Preserve all-important records in paperless court system
- Use outsourcing to ramp up quickly

### Technology Challenges

- Strengthen defenses against network threats and vulnerabilities
- Simplify and centralize security monitoring and reporting
- Reduce spam and time spent deleting it, without false positives
- Streamline provisioning of desktops
- Enhance protection for digital records
- Improve visibility into security events

### Solution

Multi-layered enterprise security solution with system and data protection from Symantec, implemented with optimal speed with help from ISH Tecnologia Ltda.

### Symantec Products

- Symantec AntiVirus™ Corporate Edition
- Symantec™ Client Security
- Symantec™ Critical System Protection
- Symantec Enterprise Security Manager™
- Symantec™ Mail Security 8260
- Symantec™ Security Information Manager
- Symantec Ghost™ Solution Suite
- Veritas NetBackup™

### Technology Environment

- Application: Custom Web-based workflow application
- Database: Oracle 9i
- Server Platform: 41 servers, most running Novell SUSE Linux, some Solaris, some Microsoft Windows®
- Storage: NetApp FAS270 NAS

### Symantec Services

- Symantec Essential Support Services

### Symantec Platinum Partner

- ISH Tecnologia Ltda. ([www.ish.com.br](http://www.ish.com.br))

### Extra Protection for Critical Servers

TJES also recently installed Symantec™ Critical System Protection on 41 servers—the Microsoft Windows-based servers that manage TJES's security solutions, and the Novell servers running Novell SUSE Linux that host the paperless document system and other critical applications.

“The servers that store or process lawsuits and everything else simply can't go down, because you could wind up delaying a case involving several judges,” Murad Filho says. “With Symantec Critical System Protection, we can protect these servers from both external and internal attacks. We can see what types of attacks are being tried and who is trying them, even in the case of internal attacks. We can implement countermeasures and even go after these people so they won't do these things anymore.”

### Gaining Visibility on the Security Landscape

“We had about 35 million security events go through these solutions in the past month,” Murad Filho says. “There were 888 incidents that came out of these events. There were about 30,000 files infected with viruses, Trojan horses, or worms. About 90 percent of the SMTP traffic was classified as spam.”

The reason he's able to reel off these numbers is that TJES recently invested in Symantec™ Security Information Manager. “With Security Information Manager, we now have great visibility of everything that is going on in the network,” Murad Filho says. The solution correlates log data from across the court's security infrastructure, and enables TJES to identify, prioritize, investigate, and respond to security threats that impact mission-critical business applications.

The product also works seamlessly with ISH whenever a problem is detected. “If there is a security incident that has been automatically classified by Security Information Manager, it will notify the team here,” says Santos. “We have one hour to go over there and do

whatever is needed to stop it or gather more information so the appropriate decision can be made. Once the decision is made, we implement security countermeasures to remediate whatever has occurred.” Afterward, using data from Security Information Manager, ISH and TJES can evaluate any further needed steps to prevent future incidents.

### Minimizing Security Administration

TJES uses Symantec Enterprise Security Manager™ software because it automates the discovery of vulnerabilities and deviations in security policies and servers across the organization, and reports results through a single easy-to-use GUI interface.

The solution also checks multiple systems simultaneously for deviations such as missing OS patches, inappropriate user password settings, unauthorized privileges, incorrect file access, changes to security settings, and incorrect configurations.

As a result, security administration has been streamlined. A five-person help desk at TJES must support 5,000 users. Before Symantec, those five people spent 80 percent of their time on security issues. Now three quarters of that time has been freed for other tasks, and the team spends only 20 percent of its time on security.

Murad Filho also reports a dramatic reduction in the time spent overseeing security, both for himself and the entire IT staff. “The whole solution has brought us more time,” he says. “In the past, IT staff spent about 35 percent of their day fixing some kind of problem related to security.”

As for Murad Filho, “Because there is a single console, I have great visibility into everything that is going on,” he says. “There's a single point where I can look at these events, instead of having to open up many different consoles.” He used to spend about four hours a day reviewing security events via the different consoles, he adds. “Now, with in Security Information Manager, I can get an overview of everything that is going on and find out if there's anything that actually needs my attention in 15 minutes.”

**“In the past, sometimes things would go out for about 12 hours and we wouldn't know whose responsibility it was to fix it. Now downtime is basically zero with response time sometimes as fast as 15 or 30 minutes.”**

**Victor Murad Filho**

IT Director

Tribunal de Justiça do Espírito Santo

**“Within 72 hours of deploying the Symantec Mail Security appliance, spam virtually stopped hitting our inboxes. Hundreds of users contacted our IT team to congratulate us and ask us what we had done.”**

**Victor Murad Filho**

IT Director

Tribunal de Justiça do Espírito Santo

## BUSINESS VALUE AND TECHNICAL BENEFITS

### Enhanced Security

- Zero downtime due to network attacks, compared to as many as 20 days a year before
- Symantec
- As many as 30,000 files with viruses, worms and Trojan horses blocked each month
- Enhanced centralized security monitoring
- Content filtering ability to stop email leakage of confidential documents

### Operational Efficiency

- 40% reduction in incoming email due to blocking spam, with virtually no false positives
- 8,000 hours in productivity gained from automatically deleting spam<sup>2</sup>
- 3,500 hours a year saved by reducing PC provisioning to 20 minutes from two hours<sup>3</sup>

### Lower TCO

- 75% reduction in security administration time
- 50% reduction in email storage due to blocking spam

### Increasing Operational Efficiency

Symantec Ghost™ Solution Suite has also freed up IT resources. By letting the team remotely deploy a PC disk image, rather than build a PC step by step, it reduces a two- to three-hour task to 20 minutes, and eliminates travel time.

The IT team saves 3,500 hours a year that are available for more valuable projects.<sup>3</sup> One of these projects is developing and rolling out a Voice over IP system, which will save TJES a projected 60 to 70 percent in telecommunications expenses,

### The Next Steps

TJES is currently implementing Veritas NetBackup™, to better manage backups across multiple server platforms, including Microsoft Windows, Linux, Sun Solaris, and VMS. “It’s all integrated with Symantec’s security solutions and storage solutions,” he says. “This way, we can see from inside Security Information Manager if our backups are being run.”

### A Partner’s Value

Murad Filho is pleased with Symantec—and has been equally impressed with ISH. “They have been indispensable in designing and implementing the solution, providing useful suggestions, giving us good support, and fast turnarounds,” he says. “ISH is one of the first companies to implement outsource security services to government agencies in Brazil. Working with them has been a great experience for us.”

<sup>1</sup> Wikipedia.Org article, “Espírito Santo”

<sup>2</sup> 4,000 email users\*5 minutes a day saved\*250 workdays a year/60 minutes = approximately 8,000 hours a year or 4 full-time staff.

<sup>3</sup> Two hours (120 minutes) reduced to 20 minutes=100 minutes saved per provisioned PC\*40 incidents a week=4,000 minutes/60 minutes per hour= 67 hours per week saved\*52 weeks=3,484 hours per year saved Travel time saved (up to one or two days per remote incident) would be additional. a