



Customer Case Study

Metropolitan Transit System Puts Privacy and Security in the Fast Lane

Montreal’s public transportation system, the STM, uses Cisco networking, security, and IP Communications technologies to deliver more secure and efficient transit services applications to over 1.3 million daily commuters.

EXECUTIVE SUMMARY

The Societé de Transport de Montréal

- Public Transportation
- Montréal, Quebec, Canada
- 7400 employees

BUSINESS CHALLENGE

- Need to consolidate and synthesize massive amounts of security information
- Need to more quickly and efficiently identify and respond to security threats
- Need to gain pervasive security intelligence

NETWORK SOLUTION

- Deployed state-of-the-art security intelligence solution
- Implemented granular monitoring of both internal and external networks
- Increased visibility into network-wide activities

BUSINESS RESULTS

- Alleviated and greatly simplified and reduced security information
- Increased speed and effectiveness of network defenses
- Effectively blocked internal network attacks and prevented widespread outbreaks

BUSINESS CHALLENGE

The City of Montréal’s transit system, the Societé de Transport de Montréal (STM), operates four subway lines, a fleet of 759 cars serving 65 metro stations, 188 bus lines, 1567 buses, and 94 paratransit minibuses across the metropolitan region, providing more than 1.3 million trips each weekday. The STM’s IT department acts as the nerve center to maintain the availability, integrity, and confidentiality of the 120 information systems deployed for this large and diverse organization. The IT department is supporting about 3000 IT users acting in 500 different functions across the company, including bus and train operators, security personnel and fire prevention workers, maintenance staff, and office workers—all of whom rely on different network applications.

“Our most important role is to unify all the applications that allow the STM to function on a single network—everything from payroll to the systems that book 3000 bus drivers on their routes each day,” says Patrick Hardy, senior network architect and administrator for the STM.

To support this massive operation, the STM has invested in a \$12 million, state-of-the-art network infrastructure, built entirely with Cisco Systems® technology. The network is extremely complex, encompassing a robust routing and switching infrastructure to support 165 servers, 6000 hosts, and more than 7400 employees. All the devices that will be used for fare collection—from turnstiles in a subway station to portable wireless ticket

validation devices—will be linked to the IP network. Twenty percent of STM buses are equipped with Cisco Aironet® wireless connectivity. The environment also includes a Cisco storage area network to support business continuity and five major IP contact centers for customer service that employ Cisco Unified Contact Center Enterprise, and handle more than 30,000 calls per day. In addition, the network data center hosts a major Web site that receives more than 1 million hits per day, supports several Web-based applications, and connects with a variety of external business partners.

In addition, payroll data and employee records traverse the network each week. With its e-recruitment applications and planned credit-card-based online ticket sales that store applicants’ personal information, the STM’s Web site also presents a highly visible target for hackers, and faces daily Internet attacks. The STM is also a public company, regulated by several municipal, provincial, and federal agencies, which require compliance to standards for data and network security and extensive reporting.

Faced with these challenges, the STM has employed state-of-the-art defenses from Cisco Systems, including Catalyst® switch-based firewall and intrusion prevention system (IPS) services, as well as the Cisco VPN 3000 Concentrator for secure remote access. But with more security devices on the network, the amount of raw security data increased exponentially. Simply identifying malicious activity in such a large network—much less responding to it—posed an enormous challenge.

“Our network registers about 5 million suspicious events every 24 hours, and 2000 incidents per day,” says Hardy. “Even after filtering out false alarms, that is still 200 events that we have to manually investigate. Before, we looked through 30-megabyte syslogs with hundreds of thousands of lines of data. The process was very slow, and often overwhelming.”

NETWORK SOLUTION

The IT team needed more efficient, proactive tools for monitoring network security information. So the STM became one of the first organizations in North America to begin using the Cisco Security Monitoring, Analysis, & Response System (MARS), a component of the Cisco Security Management Suite.

“We had a worm attack just this morning from a PC in one of our garages. Cisco Security MARS detected it immediately. The alarm went out, and the solution shut down the PC’s switch port within minutes.”

— Pierre Gingras, senior architect for Internet, intranet, and the Web

Cisco Security MARS appliances efficiently aggregate and synthesize the massive amounts of network and security data typically generated in a large enterprise network, and use sophisticated event correlation and validation intelligence to help administrators appropriately identify and respond to threats. The solution incorporates intuitive topology maps to track attacks in real time, integration with deployed network security devices to mitigate attacks in progress, intelligent rule creation and threat notification services, and comprehensive reporting systems. Together, these capabilities streamline and automate the task of identifying and responding to suspicious network behavior.

The solution also proved easy to integrate into the STM’s network and operational processes.

“The learning curve for Cisco Security MARS was very fast,” says Hardy. “It took us about 10 days to get familiar with it.”

Cisco Security MARS represented an entirely new way to manage network security information. But the fact that Cisco Systems stood behind the solution gave the STM’s IT leaders the confidence to move forward with the deployment.

“The main reason that we use Cisco products across the board is the excellent service and customer support that we receive,” says Hardy. “We also trust the performance and integration capabilities of Cisco solutions.”

BUSINESS RESULTS

Today the STM IT department can identify and respond to security threats more quickly and efficiently than ever before. These advantages translate into substantial productivity increases for the STM’s IT staff.

“Cisco Security MARS correlates all our security information extremely well, and eliminates the need to spend hours going through logs and event viewers,” says Hardy. “All the filtering, tuning, and reporting capabilities are very granular and very precise, and everything is fully automated. If the solution registers a code red event, we are paged right away, and we can take action if the solution has not already taken action for us.”

By providing a real-time picture of all activity across the network, Cisco Security MARS even offers capabilities that go beyond network security.

“Just from a networking point of view, Cisco Security MARS provides much greater visibility into the network,” says Hardy. “Other management solutions will give you a static Layer-2 map of your network. But Cisco Security MARS provides a Layer-3 topology map that allows you to see all the network devices in real time. To use a medical analogy, it is like seeing the inside of your brain, with all the nerve endings and blood flow in motion.”

PRODUCT LIST

Routing and Switching

- Cisco 7200 Router
- Cisco 2800 Routers
- Cisco 1800 Routers
- Cisco Catalyst® 6500 Series Switches
- Cisco Catalyst 3750 Series Switch
- Cisco Catalyst 3560 Series Switch
- Cisco Catalyst 2950 Series Switch

Universal Gateways

- Cisco 5300

Content Networking

- Cisco Catalyst 6500 Series Content Switching Module with SSL

Security and VPN

- Cisco Access Control servers (RADIUS, TACACS)
- Cisco Security Manager
- Cisco Security MARS
- Cisco VPN 3000 Concentrators
- Cisco Catalyst 6500 Series Firewall Services Module
- Cisco Catalyst 6500 Series IDS Services Module 2

Storage Networking

- Cisco MDS 9500 Series Multilayer Director

Voice and IP Communications

- Cisco Unified Contact Center Enterprise

Wireless

- Cisco Catalyst 6500 Series Wireless LAN Services Module
- Cisco WLSE server
- Cisco Aironet® Wireless Access Points

The solution has also greatly helped the STM IT department with regulatory compliance. Prior to CS-MARS, Hardy and his colleagues had to prepare for security audits by assembling and organizing data from various devices. The task took several days. Now audits require very little groundwork.

“We go through a security audit every year, and Cisco Security MARS’ reporting capabilities are a big help,” says Pierre Gingras, senior architect for Internet, intranet, and the Web. “In fact, we sat the auditors down in front of the Cisco Security MARS console to let them see it firsthand, and it blew them away. We got straight As. With this solution in place, audits are not really a concern for us anymore.”

With CS MARS, STM has helped ensure greater protection from both internal and external threats. If the STM network is breached, critical operational applications could be threatened, or worse disabled, thus affecting general public transit services.

“Part of the problem with the way we were handling security information before was that it focused only on external threats,” says Hardy. “It did not really look at what was happening internally—for example, if a disgruntled employee was trying to launch an attack on a server. Cisco Security MARS monitors everywhere, and gives us a complete picture of the activity on both internal and public-facing networks.”

This comprehensive visibility has already helped the STM IT team block network threats.

“We had a worm attack just this morning from a PC in one of our garages,” says Gingras. “Cisco Security MARS detected it immediately. The alarm went out, and the solution shut down the PC’s switch port within minutes. Without the solution, that PC would have likely infected the entire subnet. That is 75 PCs in that building that would have been infected within an hour. And from there, the situation would have gotten even worse.”

“Since all of our future public vending machines will be connected to the IP network, we will be technically exposed to potential threats,” says Hardy. “If hackers found a way to connect with one of those machines, they would be on our network. Having the Cisco Security MARS solution in the background to monitor and respond to all the activity, I sleep a lot better at night.”

NEXT STEPS

The STM IT team plans to continue working with Cisco Systems to enhance network capabilities and network security. Most recently, they upgraded to Cisco Security Manager to centrally provision device configurations and security policies for Cisco firewalls, VPN and IPS. The organization plans to deploy a 10 GigE Metropolitan Area Network across its subway infrastructure in the coming months, expand its use of wireless on all of its buses, and add more hotspots throughout STM facilities. The organization will also be testing the Cisco ASA 5500 Series Adaptive Security Appliances, which integrate firewall, VPN, IPS, and other security capabilities into a single, manageable platform. The STM is particularly interested in the solution’s Anti-X Module, which blocks spyware and adware.

With 20 percent of the STM workforce using mobile PCs that are more difficult to secure, the organization is also shifting its security emphasis from detection and correction to prevention. Currently, the STM is piloting the Cisco Network Admission Control (NAC) solution. When deployed, the system will provide an even greater level of security by verifying that any device attempting to access the network is properly updated and secured, and free from viruses and worms. It will also help ensure that external users (such as bus passengers) have access to only the public network.



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic
Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy
Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)