

MTR Corporation Ltd.



Merging Two Railroads While Keeping Security on Track with Symantec

To smoothly execute a merger, offset a recent fare reduction and honor a commitment to the people of Hong Kong that it will not increase fares before June 2009, MTR needed to standardize IT and become more efficient. By investing in a comprehensive security and availability solution from Symantec, MTR has been able to avoid damage from viruses and malicious code, block 30,000 attack attempts and security threats each month, improve its backup and recovery success rates to nearly 100 percent, accommodate 25 percent annual data growth without adding staff, and provide high availability for its critical document management system.

A promise to the people

Hong Kong's Mass Transit Railway (MTR), one of the most heavily used mass transit systems in the world, just got a lot bigger. In December 2007, the railway's parent company, MTR Corporation Ltd., officially merged with the Kowloon Canton Railway (KCR) with the intent to increase the efficiency of the city's transportation network. To reassure the public, MTR promised to cut fares by 10 percent the first day the merger was finalized—and freeze them through June 2009.

While the MTR will benefit from the property development opportunities and higher passenger traffic that accompany the merger, such a substantial reduction in fares has the potential to impact revenue—making it critical for the company to cost-effectively integrate the two IT infrastructures and manage them as efficiently as possible. By standardizing on Symantec security and availability solutions, MTR was able to ensure that no security disruptions, downtime, or data loss derailed its merger.

Protecting information security

In the fall of 2007, shortly after the merger was approved by shareholders and Hong Kong's Legislative Council, MTR decided to implement Symantec™ Endpoint Protection and Symantec™ Security Information Manager so it could maintain endpoint security and minimize the risk of disruption or threats to or from 12,000 employees after the merger.

Symantec Endpoint Protection provides antivirus, antispymware, firewall, intrusion prevention, and device and application control with a single agent on each endpoint and a single management console.

Symantec Global Services offered valuable expertise to help MTR get maximum values from their technology investment. Symantec Consulting Services helped MTR implement Symantec Endpoint Protection and customize the product. At MTR Symantec End-

ORGANIZATION PROFILE

As Hong Kong's leading mass transit railway transportation provider, MTR Corporation Ltd. (www.mtr.com.hk) keeps 3.4 million commuters on track every day, making the rail network one of the most densely used in the world. One of the world's few profitable public transport systems, MTR has 12,000 employees and the largest shareholder base of any company listed on the Hong Kong Stock Exchange.

INDUSTRY

Transportation

SOLUTION

Endpoint Security
Data Loss Prevention
Security Management
IT Compliance, Messaging Management
Messaging Security
Data Protection
Storage Management
High Availability/Disaster Recovery

“Symantec is one of our key strategic partners. We have been very satisfied with their service and support, and the Symantec products we use outperform similar products on the market. We are getting good value for our money with Symantec.”

M.T. Siu

IT Service Manager
MTR Corporation Ltd.

Using Veritas NetBackup, MTR has been able to accommodate a 25 percent annual growth in data volume without having to increase IT staff

“On average, we are stopping more than 30,000 threats per month on all our endpoints using Symantec Endpoint Protection.”

M.T. Siu

IT Service Manager
MTR Corporation Ltd.

point Protection supports 20 security policies written to restrict and govern employee access and behavior. Symantec Education Services provided classes for two administrators that shortened learning time and speeded up time to value. And Symantec Essential Support Services completed the solution by providing access to Symantec’s experts and product upgrades.

The company has so far been able to avoid any damage from viruses or malicious code. “On average, we are stopping more than 30,000 threats per month on all our endpoints using Symantec Endpoint Protection,” says M.T. Siu, IT Service Manager at MTR.

To monitor instances of Symantec Endpoint Protection enterprise-wide, as well as other Symantec and third-party security hardware and software solutions, MTR is using Symantec Security Information Manager. It provides a documented, repeatable process for responding to security threats and addressing IT policy compliance via a comprehensive security management program. Symantec Security Information Manager filters and correlates data from hundreds of millions of raw events—from across MTR’s network and Symantec’s Global Intelligence Network—into an actionable list of prioritized threats.

“We wanted to make sure we were protected in terms of system access, data loss, data corruption, and exposure,” says Siu. “Any merger is sensitive with regard to human resource issues. I’m not saying that people are likely to try to compromise our data, but certainly we have to protect the company against any potentially disgruntled staff. Using Symantec Security Information Manager, we can detect and investigate any unusual access activities.”

SOLUTION AT A GLANCE

Business Drivers

- Ensure data security during and after merger
- Minimize productivity loss to spam
- Improve data backup efficiency
- Provide high availability for document management system

Technology Challenges

- Simplify cross-platform data protection while accommodating rapid data growth
- Accomplish systems integration for merger on time and within budget
- Increase data backup and recovery success rates
- Reduce storage management time while increasing storage uptime
- Decrease recovery time objective (RTO)
- Support clusters in multiple data centers

Solution

Unifying multiple platforms and vendors with endpoint security, data protection, storage management and clustering

Symantec Products

- Symantec™ Endpoint Protection
- Symantec™ Security Information Manager
- Symantec Brightmail™ Gateway
- Symantec Brightmail AntiSpam™
- Veritas NetBackup™, with agents for Microsoft Exchange Server and Oracle
- Veritas Storage Foundation™ HA for Windows
- Veritas™ Cluster Server

Technology Environment

- Applications: Microsoft Exchange 2003, Oracle E-Business Suite, PeopleSoft, Open Text Livelink, BEA Tuxedo
- Databases: Oracle 8i Release 8.1.6
- Servers: 200 plus servers (HP, Sun, and Intel-based platforms) running HP-UX, Solaris, and Microsoft Windows Server
- Storage: HP StorageWorks EVA5000/8000, IBM storage area network (SAN)
- Tape Libraries: Sun StorageTek L180, Sun StorageTek L700e

Symantec Services

- Symantec Consulting Services
- Symantec Education Services
- Symantec Essential Support Services

Symantec Partners

- Ygl Consulting (www.ygl.com.hk)

“Symantec Consulting Services helped us move quickly to our new solution, allowing us to sustain growth while maintaining focus on our core business of providing excellent train service.”

Daniel Lai

Head of Information Technology
MTR Corporation Ltd.

Fighting spam on the front lines

To protect against email spam, MTR is using a Symantec Brightmail™ Gateway appliance to stop spam attacks in real time before they hit the company’s Microsoft Exchange email server. Symantec Brightmail Gateway appliances deliver antispam, antivirus, and advanced content filtering technologies to protect against inbound and outbound email and instant messaging borne threats. With structured data protection support, it enables MTR to more effectively control sensitive data, reduce risks associated with data leakage, and meet regulatory compliance mandates and corporate governance demands.

One of the industry’s most accurate solutions, Symantec automatically updates spam rules every five to 10 minutes using information from the Symantec Email Security Group which includes four operation centers and more than 2.5 million decoy email accounts in more than 20 countries. This helps Symantec respond to new spam threats as they emerge.

“With Symantec Brightmail Gateway, we have an effective and transparent solution that provides 99.999 percent protection against false positives and is 97 percent effective in filtering out spam,” says Daniel Lai, Head of Information Technology at MTR.

Backing up a mixed infrastructure

Quick, reliable backups are especially important to MTR because the company must back up its data when trains are not in service, leaving a very small backup window. Since 2002, MTR has used Veritas NetBackup™ with agents for Oracle and Microsoft Exchange Server to back up data across its HP-UX, Solaris, and Microsoft Windows platforms. Previously, the company used separate backup software for each platform, which resulted in delays and inefficiencies.

“NetBackup provides compatibility with our heterogeneous environment and is platform independent, which is even more important with the recent merger,” Lai says. “We have been able to speed time to market as a result and fully leverage our existing storage infrastructure and investment.”

Veritas NetBackup delivers complete multi-platform data protection using a single console for all backup and recovery operations. The Microsoft Exchange Server and Oracle agents simplify MTR’s database backup and recovery, providing incremental mailbox and database backups as well as full online backups, without interrupting availability of services and data to end users.

“NetBackup is a great product,” agrees Siu. “We can back up 2.2 terabytes of Microsoft Exchange data in eight hours, which is three times faster than before. We’ve also reduced our administration time because we have a single tool, from a single console, that works for all platforms. Our backup and recovery success rates are approaching 100 percent.”

MTR took advantage of Symantec Consulting Services to help migrate its storage systems to NetBackup using industry best practices and procedures. Symantec provided end-to-end support ranging from initial solution planning and design to installation and troubleshooting.

“Symantec Consulting Services helped us move quickly to our new solution, allowing us to sustain growth while maintaining focus on our core business of providing excellent train service,” says Lai. “Altogether, faster and automated backup and recovery with NetBackup has allowed us to accommodate a 25 percent annual growth in data volume without having to increase IT staff or shift IT resources.”

BUSINESS VALUE AND TECHNICAL BENEFITS

Endpoint Security

- 30,000 attack attempts and threats blocked each month
- No infections or damage from malicious code
- 95% accuracy in filtering spam with virtually no false positives

Data Protection

- Threefold faster email backups
- Reduced backup administration time through single management console
- 99.95% backup success rate
- 100% recovery success rate
- Recovery time objective (RTO) of less than 10 minutes achieved

Operational Efficiency/ Savings

- 33% hardware cost avoidance because of clustering flexibility
- Ability to grow disks dynamically with no downtime
- 25% annual growth in data accommodated with no increase in staff or backup window

Simplifying storage management

To manage its storage environment without requiring interruption to servers and critical applications, MTR uses Veritas Storage Foundation™ 5.0 High Availability for Windows. By creating virtual storage devices from physical disks and arrays—allowing storage to be optimally configured and shared—Veritas Storage Foundation brings advanced online storage management to Microsoft Windows Server environments. “The ability to grow or partition disks on the fly is a great feature,” says Siu. “We can make changes in minutes that would take hours in planned down time without Storage Foundation.”

Ensuring high availability

MTR is using Veritas™ Cluster Server to provide high availability for its corporate document management system. The company uses a 3:1 local cluster architecture, with three servers failing over to one standby node, instead of the more common 1:1 active to passive clustering architecture. Because Veritas Cluster Server allows true N+1 “roaming spare” capability, without requiring a dedicated spare server per application MTR has been able to purchase four instead of six servers, reducing hardware costs by 33 percent.

“Right now it only takes two to 10 minutes to failover to a standby node with no data loss—which is fantastic. And because it is a cross platform solution, we have the flexibility to change hardware vendors without having to retrain our employees or substantially change our HA/DR solution. We may need to extend the local cluster to stretch between different data centers as a result of the merger, and Veritas Cluster Server will allow us to do that,” says Siu.

A trusted partner for a comprehensive security and availability solution

By standardizing on Symantec for data center management and security solutions, MTR has saved time and money. But just as important, MTR has a partner it can trust.

“Symantec has a complete understanding of our data protection needs, strong security products, and a strong commitment to our business,” says Lai. “With Symantec, we have a total comprehensive security and availability solution that has delivered cost savings, business continuity, and helped with our compliance efforts.”

“Symantec is one of our key strategic partners, and plays an important role in our business,” concludes Siu. “We have been very satisfied with their service and support, and the Symantec products we use outperform similar products on the market. We are getting good value for our money with Symantec.”