

**Location: Miami, FL, USA**

**Sites:** More than 400: 367 schools plus district offices and service facilities

**Users:** More than 400,000: 362,000 students, 21,000 teachers, 28,000 staff

**Industry:** Education

**Value-Added Reseller:** United Data Technologies

**Applications:** Online instruction, testing and record keeping; Gradebook; Cognos facility database; terminal emulation; web portal, web and email; network security and management



## Miami-Dade School District Pinpoints Vulnerabilities, Increases Network Security and Availability, Improves Productivity



### CASE STUDY

#### IN BRIEF

##### GOAL

- › Protect District WAN and LAN assets from both internal and external threats
- › Free bandwidth for District applications
- › Prepare network for future growth, applications, and security threats
- › Centralize, simplify and speed management of network security

##### SOLUTION

- › 3Com® Intrusion Prevention System technology
- › Deployment and support by United Data Technologies

##### RESULT

- › Secure network—superior to the security of most banks—with highly advanced technology and multilayer architecture
- › Better applications performance; reclaimed bandwidth that had been lost to security exploits and management overhead
- › Scalable, flexible security infrastructure that can be updated dynamically with quick and easy deployment
- › Higher IT staff productivity that results from proactive, centralized security management

## Snapshot

In the network security realm, being bigger does not necessarily mean better. It can mean increased exposure. In the case of Miami-Dade County Public Schools, the fourth largest U.S. school district, the District network draws hackers from around the world. Still more vulnerabilities arise from the network's 400,000 authorized users. Prior to 2007, the network experienced frequent denial of service (DoS) attacks, applications performance delays and downtime that lasted for hours. Although it used firewalls and intrusion detection systems, anti-virus and content filtering software and a variety of management tools, the security was insufficient. Some big ideas from the District's small Network Services department—and a two-inch-tall 3Com® technology platform—solved the problem. The District network is now protected by a multilayer security architecture, based on 3Com intrusion prevention technology and security management systems.

#### CHALLENGES

The District realized that to better secure its network, it would have to address these major technology and business challenges:

**A passive legacy.** "The essential technology problem was that our network security was passive, or reactive, so it could only detect a problem after it was on our LAN or WAN," says Thomas T. Sims, director of network services. It could not block or quarantine infected devices, causing entire LANs to be shut down and unavailable until the irritant was cleansed and the network tested fit for operation to resume.

**A big target.** The District has a large network and one of the world's largest web portals. It attracts scanning and exploits by external hackers (many of them in Asia) and internal hackers (many of them students). "It's amazing what students today can do when they have time on their hands," says Sims. "They are curious, like a challenge, and try to use the desktops at school and passwords from home to beat our system." Networks can inadvertently launch infected applications or spyware when doing peer-to-peer downloads, and users sometimes bring compromised devices to school and plug them into the network.

**Decentralized control.** The District has two physically distinct networks, both served by one Metro Ethernet Native Mode LAN Interconnection WAN. One is the district-wide staff and teachers network, which relies on

“It’s the ideal solution for the District—an inline device that’s easy to use and manage, scalable, and extremely effective—no wonder Gartner put 3Com in its ‘Magic Quadrant.’”

Gerard Amaro,  
Vice President,  
United Data Technologies

“Prior to the 3Com solution, we would have to shut down the school’s entire network, penalizing thousands of users.”

Thomas T. Sims,  
Director of Network Services  
Miami-Dade County Public Schools

“The garbage traffic is gone and the new security platforms and SMS present no overhead issues. We’ve had no negative impact or compromised bandwidth at the core, sites, or any of our segments.”

Benito Horta,  
Network Security Analyst,  
Miami-Dade County Public Schools

applications servers at the central site. The other comprises all LANs—based largely on 3270 terminal emulation to mainframes at the central site—used by the 367 schools for students. At each school site the principal, assisted by the school’s site technician (“Tech”), controls the LANs sitting behind the WAN router.

**Limited resources.** The Network Services Department is a small group with big responsibilities. The 11-person team is charged with managing, servicing and securing the District’s core network and WAN, which serves 90,000 desktops at more than 400 sites. Its network security analyst, Benito Horta, is responsible for managing all the security devices; remediating desktops and servers that experience problems; enforcing compliance with district security policies, software patches and upgrades; and scanning and monitoring the security of the network. But the decentralized district network and hodgepodge of security management tools meant that Horta actually had to spend most of his workdays just reacting to security breaches.

### WHY 3COM

In late 2005, Sims and Horta sought new network security solutions from a range of vendors, and in 2006 began evaluating and field-testing them. “I’m a big believer in ‘show me,’” says Sims. “I’ll only buy a solution that we’ve run on our network for 30 to 90 days.” United Data Technologies (UDT), the District’s network VAR, facilitated the evaluations. “We rely on UDT for many solutions—they are more like a partner than a vendor, and are very responsive to our needs,” Sims says. The result of the District’s proof-of-concept testing: “3Com’s solution was superior in four ways: its advanced technology, scalability and flexibility, performance and simplified central management,” says Sims. “The 3Com® technology is clearly best of breed.”

After installing IPSs in the core, UDT technicians led by Horta in 2007 began deploying X-Family Integrated Security Platforms at the schools. These products integrate an intrusion prevention system, high-performance firewall and IPsec VPN, web content filtering, traffic shaping, dynamic and multicast routing, and industry-leading protection for an unlimited number of users. “It’s the ideal solution for the District—an inline device that’s easy to use and manage, scalable, and extremely effective,” says Gerard Amaro, UDT vice president. “No wonder Gartner put 3Com in its ‘Magic Quadrant.’”

### INCREASED SECURITY PASSES PENETRATION TEST, DOES NOT STEAL BANDWIDTH

The District takes advantage of many of the X-Family platforms’ integrated capabilities, including web content filters, quarantine, firewall and Digital Vaccine® updates. The solution resolves the District’s biggest vulnerability—threats emanating from school sites, which quickly become a two-pronged attack on the LAN and WAN. “By placing an X-Family platform at each site, we stop threats at the school’s router, before they get onto the WAN,” says Sims.

When a PC is misused or infected, the solution’s Security Management System (SMS) quarantines and shuts down the PC, and sends an IP address alert so the issue can be fixed. “Prior to the 3Com solution, we would have to shut down the school’s entire network, penalizing thousands of users,” says Sims. Another way the solution improves instruction: “We’re catching kids at classroom computers who hoodwink their teacher into thinking they’re working, but they’re actually playing games,” says Sims. “Remotely from any of our SMS screens, we can see everything they’re doing.”

Before the 3Com deployment, students downloading newly released music and games would absorb 100% of their school’s LAN bandwidth. Now with the 3Com solution, the bandwidth is freed. “The garbage traffic is gone,” says Horta. “And the new security platforms and SMS present no overhead issues. They don’t produce false positives. We’ve had no negative impact or compromised bandwidth at the core, sites, or at any of our segments.”

Horta uses the Digital Vaccine service to regularly update security filters to ensure the District’s network security is dynamic and protected against new attacks. This 3Com service automatically distributes updated signature, vulnerability, protocol anomaly and traffic anomaly filters to customers’ X-Family devices for pre-emptive protection against new and zero-day vulnerabilities. It also offers web content filtering, telephone technical support, advance hardware replacement and software updates for X-Family security platforms.

To assess the strengths and vulnerabilities of its network security, the District annually contracts a third party to conduct a blind penetration (pen) test. The testers use hacking tricks to break into multiple areas of the network. “With the X-Family in place, we got a very impressive pen rating,” says Sims. “The testers told us our District is better secured than most banks.”

“With the X-Family in place, we got a very impressive pen rating. The testers told us our District is better secured than most banks.”

Thomas T. Sims

“A big differentiator of the 3Com solution is its huge built-in functionality. A single X-Family platform can do VPN tunnels, content filtering, quarantining, traffic shaping, and more. We have all the capabilities we need now and for the future, in one box.”

Thomas T. Sims

### **SOLUTION IS SCALABLE AND FLEXIBLE; DEPLOYMENT IS FAST, NON-DISRUPTIVE**

“A big differentiator of the 3Com solution is its huge built-in functionality,” says Sims. “A single X-Family platform can do VPN tunnels, content filtering, quarantining, traffic shaping, and more. We have all the capabilities we need now and for the future, in one box.” The solution handles a wide variety of mission-critical District applications, including Gradebook, Cognos, the website, and Microsoft Exchange email.

About 10 schools a week get an X-Family platform, “and the deployment does not disrupt school operations at all,” says Sims. “The 3Com platforms are very easy and fast to deploy,” Horta says. He explains his process: a Tech connects the X-Family platform at a school site and boots it up; from elsewhere Horta uses the web-based SMS interface to add the school group, push out the District’s security policies and verify the functionality. “Altogether the deployment is done within 45 minutes,” says Horta. “We’ve already deployed about 200 schools, and expect the rest to go just as quickly and smoothly.”

### **MANAGEMENT SYSTEM IMPROVES PRODUCTIVITY, ENABLES STRATEGIC WORK**

The comprehensive and centralized capabilities of the SMS have revolutionized the District’s management of its network security, transforming it from reactive to proactive. Network Services staff now have the ability and time to monitor network use, see packet captures at a glance, and preemptively identify suspicious activity. “The 3Com solution is a very efficient way for us to do things,” says Sims.

Prior to its deployment, the District used a variety of tools for security management. “They generated a lot of false positives. It was also extremely hard to get data that could be correlated,” says Horta, who reports that he found himself spending 90% of his work hours on “managing the management product” and reacting to security breaches.

Sims reports that on average more than half of his department’s labor time—and much of the school Techs’ time—was spent responding to security breaches and the outages they caused. “With the X-Family solution, our District is saving tens of thousands of dollars weekly daily in labor costs,” says Sims.

The SMS and X-Family solution helps the schools to quickly and efficiently resolve most security problems themselves, rather than require assistance from Network Services. It immediately alerts the school site’s Tech of the local IP address problem and quarantines the device until it is remediated. It’s no longer necessary to shut down the school site’s network. “It takes us totally out of the response dispatch mode,” says Sims. “It has wound ‘windshield’ [driving] time way down.”

The district has deployed SMS solutions in regions of its physical network, operator consoles at the sites and a management console for Horta. The management systems let Horta create and enforce security policies, manage the devices and their groups, implement and release quarantines and help operators foresee problems. “I really like the very, very intuitive SMS interface—it does the job and gets out of your way,” says Horta. “I create a policy, and that’s it; there’s no need for us to micromanage it. SMS is smart and preemptive, lets us act strategically, and saves us all a lot of time. I also like that it doesn’t require a bunch of servers—you just plug in the box. It’s very impressive management technology, especially for such a large number of devices,” he says.

### **LOOKING AHEAD**

The District intends to test the new 3Com X5 Unified Security Platform, a smaller version of the X505 platform. Cooled by convection, it eliminates fan noise. The District will evaluate it for use in older school sites that lack a wiring closet or require deployment in an office.

Network Services staff also plan to implement more of the advanced capabilities built into the X-Family platform. One of the first: using traffic shaping to prioritize applications.

“We’re always open to new technologies, and the X-Family is a key new technology,” says Sims. “We’re very impressed by the 3Com solution. It brings us a lot of ‘bang for the buck’.”



**LEARN MORE: Visit [www.3com.com/case\\_studies](http://www.3com.com/case_studies).**

3Com Corporation, Corporate Headquarters, 350 Campus Drive, Marlborough, MA 01752-3064  
3Com is publicly traded on NASDAQ under the symbol COMS.

Copyright © 2007 3Com Corporation. All rights reserved. 3Com, the 3Com logo and Digital Vaccine are registered trademarks of 3Com Corporation. All other company and product names may be trademarks of their respective companies. While every effort is made to ensure the information given is accurate, 3Com does not accept liability for any errors or mistakes which may arise. All specifications are subject to change without notice.

505408-001-001 06/07