


**CUSTOMER SUCCESS**

# Complete Visibility, Security and Application Performance Control



**CUSTOMER:**  
 Hillside Board of Education  
 New Jersey, USA  
 (3400 Students, 7 Campuses)

**CYMPHONIX PRODUCT:**  
 Network Composer NC1500

**SITUATION**

Hillside School District in New Jersey is a specialization-focused public school district comprising preschool through college-prep programs. With over 3,400 students and seven separate campuses district technology administrators are tasked with maintaining productive data flow for students and faculty while protecting them from threats.

In addition to managing traditional networking challenges the Hillside technology administrators were faced with slow Internet response times, spyware and virus infected machines, content-filtering service fees, and illegal peer-to-peer content downloads. In 2004 district budgets began to be impacted as administrators were forced to pay for overages just to keep Internet connectivity fast enough for mission-critical applications.

**CHALLENGE**

Hillside needed a solution to protect critical network resources and give priority to district applications. The district's technology administrators had several priorities for any new solution. First, they needed visibility into what was actually going on with their Internet traffic. They needed to understand which computers were

monopolizing Internet resources and why. So, by understanding Internet traffic administrators hoped to accurately forecast the amount of bandwidth the district would need in order to remain productive and still avoid budget-taxing overages. Also, by gaining visibility they hoped to be able to prove or disprove the need for an infrastructure upgrade. Second, they needed to identify which threats they were facing and which computers were already infected. By identifying threats proactively administrators could implement strategic security solutions to stop infections from entering the network. Finally, they wanted a solution that would allow them to automatically block various threat types and prioritize valuable Internet usage.

Hillside evaluated numerous threat management solutions including router upgrades, managed services, and add-on solutions to their current hardware. None of these solutions would provide them with the visibility, protection, and performance improvement they needed. Even unified threat management converged appliances fell short of their requirements – they provided the security component, but could not deliver the visibility or application performance control the district needed.