



## **CONSENTRY NETWORKS ENABLES IDENTITY-BASED CONTROL FOR TEXAS SCHOOL DISTRICT**

### ***Mount Pleasant Independent School District Improves Security and Availability with ConSentry Solution***

**Milpitas, CA –November 13, 2006** – ConSentry Networks, a leading provider of secure LAN solutions, announced today that the Mount Pleasant Independent School District of Mount Pleasant, Texas, is using the ConSentry LANShield platforms to detect and stop unauthorized activity and to prevent the spread of malware.

The Mount Pleasant School District is a K-12 school system that encompasses about 5,000 students and 900 employees spread across eight sites. Although the district's LAN was protected at the perimeter by an intrusion prevention system (IPS) as well as by anti-virus software, the district had no way to control user access on the LAN or to monitor and control how network resources were used. The school district also needed a better way to contain malware, since IPS devices are too expensive to deploy throughout the internal LAN segments. A three-year search for an easy-to-use, affordable LAN security solution that could track and control traffic on the network ultimately led to ConSentry Networks.

"The ConSentry LANShield devices are a great complement to our other security solutions," said Noe Arzate, systems administrator at the Mount Pleasant School District. "The admission control and captive portal features let me control who gains access to the LAN. But I also need to limit what users can do on the LAN, so the post-admission control is critical. For example, I now can make sure that only teachers and key administrators have access to the grading system, and guests and contractors are restricted to Internet access. The visibility the LANShield provides shows me what users did and how and when they did it, so I can correct any problems that may have caused a security breach."

A Layer 2 through 7-aware device, the LANShield device operates inline, giving it complete visibility into LAN traffic. Arzate can thus define a range of access control policies based on MAC and IP addresses, applications and content at Layer 7 and above, users and roles, and

more. ConSentry's patent-pending malware algorithms detect zero-day attacks and let IT define policy to block just the infected application or all traffic from the affected user.

"Teachers lose a lot of time when they don't have a computer," said Arzate. "They can't put grades in, and they don't have the resources to provide instruction." The improved uptime from blocking malware, together with reduced troubleshooting due to increased LAN visibility, directly and positively impact the district's education mission.

The ConSentry LANShield devices have already proven their worth, enabling Arzate to see computers generating unnecessary traffic inside the network. He also used LANShield to pinpoint a vulnerability scan attack. The IPS identified a printer as the source of anomalous traffic, but the LANShield device showed that a computer connected to the printer was actually the source—it was using the printer to scan for open ports on other systems.

The ability to simply drop the LANShield device into the network was another major draw for the Mount Pleasant ISD. "Being a school district, funds are limited, so the fact that we were able to just switch a couple of patch cables and have the system up and running without any reconfiguration is a big plus," said Arzate.

Initially the school district used the LANShield visibility function and malware controls, and then the district implemented simple access control policies. More granular policies will be implemented in the future, with more restrictions on student accounts.

"It's satisfying to see the Mount Pleasant ISD benefit from the controlled network use, improved system availability, and reduced troubleshooting costs ConSentry enables — all key elements given the budget and staff restraints typical in education," said Dan Leary, ConSentry Networks' vice president of marketing. "Most important, improved LAN security translates into better instruction, and ConSentry is excited to be part of such an important mission."

### **About ConSentry Networks**

ConSentry Networks delivers comprehensive LAN security, enabling businesses to protect their corporate assets, ensure continuity of operations, and dramatically reduce the risk of security breaches. ConSentry enables this pervasive security while lowering IT's cost of operations through its flexible, high-performance platform powered by ground-breaking custom silicon and revolutionary LAN security software. Backed by blue-chip venture capital firms that include Accel Partners, DAG Ventures, INVESCO Private Capital, and Sequoia Capital, ConSentry is headquartered in Milpitas, California.

*ConSentry Networks, the ConSentry Networks logo and LANShield are trademarks of ConSentry Networks Inc., for use in the United States and other countries. All other product and company names herein may be trademarks of their respective holders.*