



*ConSentry provided the Council with a cost-effective and comprehensive LAN security platform that fulfills its LAN admission and access control requirements and enables it to enforce its security policies.*

## Conseil des écoles publiques de l'Est de l'Ontario

The Conseil des écoles publique de l'Est de l'Ontario struggles with several issues common to educational institutions and school boards in particular. The network supports a broad range of user types as well as a mix of managed and unmanaged laptops and PCs. In addition, students on the network use their laptops for gaming and other activities that IT worries could leave those machines particularly vulnerable to malware infection.

In the board's network, the main resources are all located in a centralized core. Enforcing who can access the resources in that core and protecting against the spread of malware were the Council's main LAN security concerns. Specifically, IT needed to:

- ◆ perform host posture check on managed and unmanaged machines
- ◆ provide role-based access to resources, separating access for students vs. faculty and staff
- ◆ contain the spread of malware

### TECHNOLOGIES CONSIDERED

The board considered deploying host-based agents for scanning machines to perform posture check. However, these solutions fell short in two critical areas for the board. First, that approach would require IT to install software on every desktop to perform the check. In addition to being a significant burden on IT's limited resources, this approach also provided no means for scanning unmanaged machines – the personal laptops of students and faculty that comprise the majority of network devices.

Second, those host-based agents could not support any kind of control over what resources users could reach and transactions they could perform after they were admitted onto the LAN. That kind of post-admission control – ensuring students could not access the grading system, for example – was essential to protecting the board's LAN and LAN-based resources.

### THE CONSENTRY ALTERNATIVE

The board selected ConSentry Networks to provide its LAN security. The ConSentry LANShield platform enables:

Conseil des  
écoles publiques  
de l'Est de l'Ontario



### About Conseil des écoles publique de l'Est de l'Ontario

The Conseil des écoles publiques de l'Est de l'Ontario serves more than 11,000 students in 37 elementary schools and high schools located throughout Eastern Ontario Canada.

### The Challenge

This school board had no means of checking desktops for the presence of adware or spyware or controlling where students and faculty can go on the LAN.

### The ConSentry Solution

The ConSentry platform provides the board with a simple means of performing posture check, with a dissolvable agent that can operate on managed and unmanaged machines. In addition, ConSentry ensures that no student traffic can access such core resources as the grading system.

- ◆ Network Admission Control (NAC) – authentication and posture check to control who can enter the LAN
- ◆ Visibility – incident- and exception-based information at Layer 7+, tied back to the user
- ◆ access control – role-based provisioning to control user activities on the LAN
- ◆ Threat control – block propagation of worms and other malware to prevent network meltdown

The ConSentry platform provides these key security features while maintaining LAN-speed throughput and without requiring any changes to the LAN.

The Council has deployed the ConSentry LANShield platform to scan machines and protect its centralized resources. The ConSentry platform sends a dissolvable agent to all machines to scan for compliance with OS and AV levels and check for the presence of any adware or spyware.



Also, staff and faculty authenticate to Active Directory, and ConSentry allows those users onto the LAN following their successful authentication and applies the appropriate access permissions based on their faculty status. The ConSentry platform ensures that students, on the other hand, gain only limited access to LAN resources and that traffic from them is not allowed to reach the protected core. The Council also relies on the ConSentry platform to protect against zero-hour threats, tracking usage for traffic anomalies and blocking any detected malware.

ConSentry provided the Council with a cost-effective and comprehensive LAN security platform that fulfills its LAN admission and access control requirements and enables it to enforce its security policies.

#### ABOUT CONSENTRY NETWORKS

The ConSentry Networks Intelligent Switching architecture delivers native user and application control at the LAN access edge. With this technology, ConSentry’s award-winning LANShield switch product family enables IT managers to improve the visibility, control, and performance of users and applications and radically simplify security, LAN deployment and operations. ConSentry is backed by blue-chip venture capital firms Accel Partners, DAG Ventures, INVESCO Private Capital, and Sequoia Capital and is headquartered in Milpitas, California.

**Corporate Headquarters**  
 ConSentry Networks  
 1690 McCandless Drive  
 Milpitas CA 95035  
**Phone** 408.956.2100  
**Fax** 408.956.2199  
**Toll-Free** 866.841.9100  
 Email [info@consentry.com](mailto:info@consentry.com)  
[www.consentry.com](http://www.consentry.com)

**Worldwide Locations**  
 London, United Kingdom  
**Phone** +44 (0) 00870 351 9494  
 Frankfurt, Germany  
**Phone** +49 69677 33 4  
 Tokyo, Japan  
**Phone** +813 5532 7630

For a complete listing of all our office locations go to:  
[www.consentry.com/company.html](http://www.consentry.com/company.html)