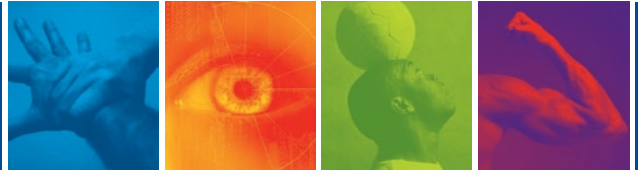


# Addressing the Top Security Concerns for K-12 School Districts



We've all seen the news stories. A high school is embarrassed when news hits that one of its students had a little side business going, getting paid to change students' grades in the school's system. A teacher transfers some student records off a home computer and takes down the district network, having unleashed a worm off the unpatched laptop.

K-12 districts, while benefiting enormously from increased adoption of technology, also find themselves increasingly vulnerable to network security issues.

## The key challenges include:

- **Data protection** – schools must avoid violating FERPA and HIPAA, most seriously, but also must protect against accidentally releasing other sensitive student information such as alternative assessment records or basic directory information
- **Traffic segmentation** – student applications and traffic should not mix with those of faculty and staff – traffic from student labs, for example, should never reach administrative offices
- **Malware containment** – viruses and other attacks can impact records, disrupt lessons, prevent web postings of lessons, and cause teachers to lose instructional time – staff or student laptops coming in from home pose an especially high risk
- **Secure wireless connections** – wireless greatly enhances productivity, but assets on the LAN must be protected from wired or wireless attacks
- **Investment protection** – many school districts have been able to secure grants and other state funding to purchase laptops and desktops, and these systems need to be protected against infection and the spread of malware



In addition to these technical issues, K-12 districts operate under the additional constraints of limited budgets and resources. So along with resolving these security-based problems, any technical solution must provide a simple, transparent means of deployment.

A variety of tools are needed to address the full scope of K-12 district challenges. Fundamentally, layering additional security into the fabric of the network provides the broadest set of security capabilities.

## The capabilities needed to secure K-12 districts include:

### Role-based access control.

People should gain access to information only on an as-needed basis. Only users in a teacher or administrator role should be able to access the grading system, for example, and only staff in an administrator role should be able to access a payroll system. Having users and their roles in an identity store, such as Active Directory, should be the basis for enabling this role-based access control.

### Full separation of traffic.

The ability to define network zones, by server type for example, and designate which user roles can access those zones, enables IT to appropriately separate administrative from student or lab traffic. For example, a district should be able to block traffic for anywhere outside the administrative offices from reaching payroll, grading, or other sensitive systems.

### Detecting and blocking malware.

LAN security includes protecting the availability of the LAN itself, so a security device should be able to recognize threats, even zero-day threats, and contain them at the source. This type of malware containment must go beyond what anti-virus or perimeter protection devices do – it must continuously monitor traffic, looking for anomalous behavior, and have the ability to immediately block that infected traffic.

## Application visibility and control.

Peer-to-peer and file-sharing applications can wreak havoc on a district network. The ability to detect and block those applications is critical for maintaining network performance and uptime and for preventing inappropriate network usage. Plus, students shouldn't be accessing inappropriate websites, so tracking which URLs LAN users are reaching is key. In addition to controlling for acceptable use policies, this kind of LAN insight is critical to troubleshooting network incidents and maintaining uptime for teaching.

## Time-of-day or location-based access control.

To augment standard role- or identity-based access control, districts need the ability to control access by time of day or by location. For example, a district might set a policy that the grading system can be accessed only during school hours, so a student attempting to hack it over the weekend could not successfully penetrate it. Similarly, a district could decide that the student directory information should be accessed only by onsite personnel, so someone attempting to reach that information over the Internet would be blocked.

## ConSentry Helps Secure K-12 Districts

ConSentry enables school districts to control who is allowed onto the LAN, restrict what students and staff can do on the LAN, and prevent threats from disrupting network services or compromising data.

The ConSentry LANShield devices provide holistic, integrated security in platforms that easily integrate into existing networks. The LANShield Controller drops into any LAN infrastructure, sitting between wiring closet switches and the core. The LANShield Switch is a wiring closet switch, offering gigabit links to desktops.

Both platforms provide the full set of capabilities needed to protect school district assets:

- **Network Admission Control (NAC)** – authentication and posture check to control who can enter the LAN
- **visibility** – full logging of all LAN traffic, including Layer 7 information such as application name or even file name, all tied back to the user
- **identity-based 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 LANShield devices provide all this capability in a single platform, and it requires no client software, no changes to the LAN infrastructure, and no modifications to the existing identity stores. IT can validate the security posture of endpoints using the ConSentry dissolvable agent that downloads over a web browser connection, so no software installation is needed. ConSentry provides full policy creation and distribution, as well as complete LAN visibility and simplified incident response, in its InSight Command Center. And ConSentry's ability to enforce access policies, while maintaining gigabit speeds, derives from its custom silicon that performs the deep packet inspection needed to secure every flow on the LAN.

Learn more about ConSentry, and learn how to secure the district network without burdening the IT staff, the teachers, the administrators, or the students.

## About ConSentry Networks

ConSentry Networks delivers a holistic approach to LAN security. We take you beyond NAC by providing identity-based access controls, zero-day threat containment, and Layer 7 visibility that fits into your existing LAN without a redesign or upgrade. Simple, economical, and wire-speed.

Founded in 2003, ConSentry is based in Milpitas, California and has received funding from Accel Partners, DAG Ventures, INVESCO Private Capital, and Sequoia Capital. For more information visit our website [www.consentry.com](http://www.consentry.com).



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

**Germany**  
ConSentry Networks  
Lyoner Strasse 6 D-605 8  
Frankfurt Germany  
**Phone** +49 69 677 33 4  
**Fax** +49 69 677 33 00

**United Kingdom**  
ConSentry Networks  
Lakeside House 1, Furzeground Way  
Stockley Park, Heathrow, UB11 1BD  
**Phone** +44 (0) 2086 22 3020  
**Fax** +44 (0) 2086 22 3200

**Japan**  
ConSentry Networks  
Hibiya Central Bldg. 14F  
1-2-9, Nishi Shinbashi, Minato-ku  
Tokyo 105-0003 Japan  
**Phone** +813-5532-7630  
**Fax** +813-5532-7373