Nevis NETWORKS

Customer Case Study

Upper Canada District School Board Selects Nevis to Secure 100+ Schools

UPPER CANADA District School Board

> ***"We needed a solution to reduce the risk of threats gaining access and spreading within our network -- without the need to install client-based software. After evaluating other security solutions, we selected Nevis' LANenforcer as the best solution to meet our needs."***
>
> -- *Jeremy Hobbs, Chief Information Officer*

Supporting over 40,000 student, teacher, and staff users in their environment, Upper Canada District School Board (UCDSB) needed a cost-effective way to ensure appropriate access controls for their mixed user community – which spans across more than 100 schools. The UCDSB provides public Internet access, library and class resource access as well as controlled access to confidential data such as student records and financials. UCDSB was challenged with finding a cost-effective way to centrally manage, enforce, and audit access control based upon the identity of a user. In addition, mitigating malware risks posed by unmanaged, student-owned laptops and PCs was another critical initiative for the school board.

About Upper Canada District School Board (UCDSB)

The Upper Canada District School Board is one of the largest public school boards in Ontario, Canada and is responsible for supporting 100 K-12 schools with approximately 35,000 students and 5,500 staff. It serves as the central decision and financial body for assuring quality education for all students.

Key Challenges

Many of UCDSB's users connect to the network using laptops and PCs that are not managed by the IT staff. Unmanaged endpoints pose significant risks to network availability and data integrity and confidentiality since the IT staff is not fully aware of the security posture of these hosts. In fact, several cases of malware infections have caused network disruption and downtime as well as administrative headaches for the UCDSB team – highlighting the need for persistent threat detection and containment.

Additionally, open access for many different types of user profiles (students, teachers, administrators, support staff,…) introduces complexity into the access control policy enforcement process. For example, students should be given open access to shared resources such as the Internet, classroom applications and library databases. At the same time, access to sensitive data such as student records and financial data must be tightly controlled and constantly monitored.

Managing costs while meeting these challenges was a top priority. Additionally, maintaining user productivity was a key requirement as well, as school administrators and teachers – often connecting remotely – need to access critical data resources to fulfill their responsibilities to the student community.

Nevis' Solution for UCDSB

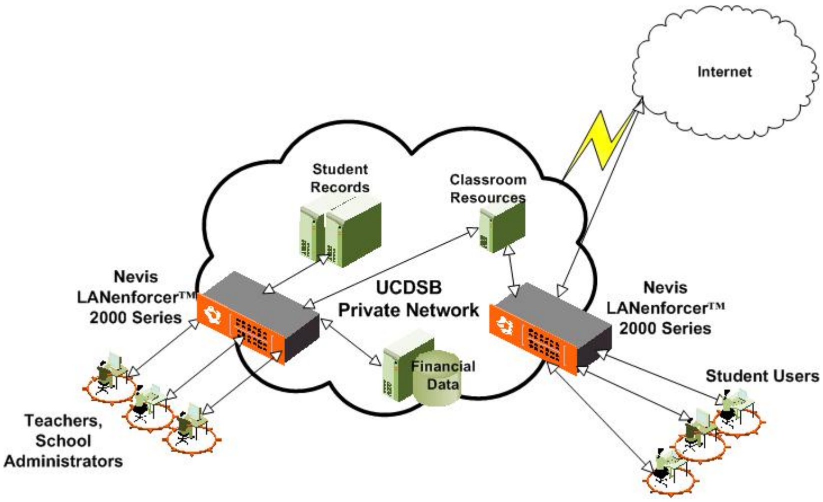
Deploying a NAC solution was a critical first step in UCDSB's LAN security strategy. However, UCDSB realized the need for more comprehensive LAN security protection – *before*, *during*, and *after* network access is granted. As a result, UCDSB selected the Nevis LANenforcer LAN security solution to satisfy both pre- and post-authentication NAC functionality requirements as well as advanced threat detection and continuous access control policy enforcement.

Specifically, by implementing LANenforcer, UCDSB has achieved the following benefits:

- Automated user identity-based access control policy enforcement
- Greater user visibility and accountability
- Endpoint integrity verification – before, during, and after users connect
- Multi-layered threat detection, control and containment
- Centralized policy management and configuration

Open Access Meets Identity-Based Access Control

The Nevis LANenforcer 2024 transparent security appliances enforce granular, identity-based access policies for each of the UCDSB users. Teachers, school administrators and students are only given access to those resources that are appropriate for their responsibility profile. Detailed reporting allows IT staff to monitor user activity and verify the integrity of student records and other sensitive data.


Internet
Student Records
Classroom Resources
Nevis LANenforcer™ 2000 Series
UCDSB Private Network
Nevis LANenforcer™ 2000 Series
Financial Data
Student Users
Teachers, School Administrators

Additionally, endpoint assessment is performed before, during and after users attempt to connect to the network – so risks associated with unmanaged endpoints are significantly reduced.

Network infrastructure protection and availability is continually assured through LANenforcer's persistent threat detection functionality. Malicious code threats are now detected and contained immediately via multiple detection techniques such as anomaly detection, a stateful firewall and LAN-optimized IPS.

> ***"Both students and staff are regular users of our network which creates a challenge to assure appropriate access to data. We provide public Internet access, access to library and class resources, and controlled access to confidential data such as student records and financials within our private network. Nevis allows us to easily and cost effectively manage, enforce, and audit access control based upon the identity of a user."***
>
> *-- Jeremy Hobbs, Chief Information Officer*