

Educational institutions face an increasingly unique, and menacing, security challenge – providing open and readily available network access to students, faculty and staff while maintaining high levels of security to prevent breaches of personal data and network degradation. Simultaneously, educational IT must balance these security concerns with the daunting challenges of meeting state and federal mandates, including PCI, SOX, HIPAA, FERPA, SPA and more.

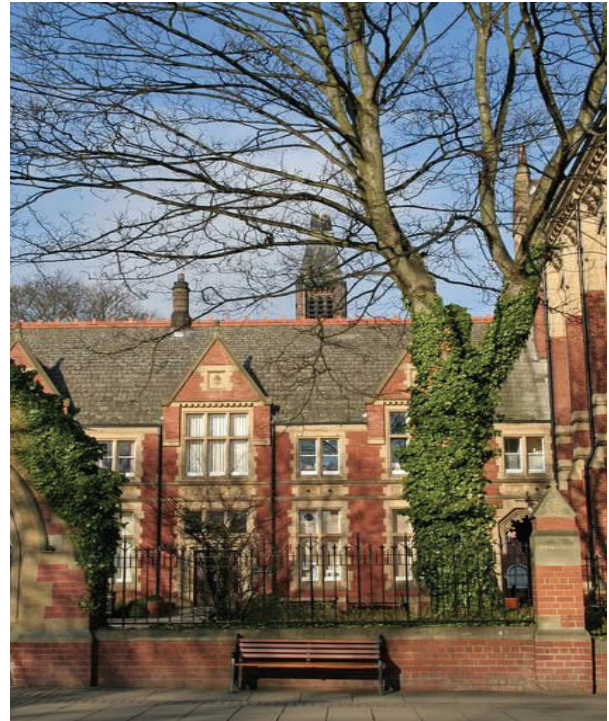
The threat landscape facing educational institutions has evolved – no longer are the only concerns network attacks from the outside world. Network administrators are faced with an increasingly high number of threats resulting from the actions of students and faculty themselves from inside the network, including:

- E-mail based phishing and malware attacks
- Program downloads from popular Web 2.0 and social networking sites
- Infected foreign devices connecting to the network
- Increased use of peer-to-peer (P2P) file-sharing networks, which lead to the spread of malware and potential copyright violations

Sharing media files and downloading internet content makes the whole network vulnerable – exposing it to intrusions, worms, viruses, malware and other hacker attacks. Once introduced into the network, these various forms of malware can lead to severe data breach – including loss of personal and financial records – or result in the complete collapse of the network.

With potentially thousands of students and faculty accessing the network with little regulation, how can IT staffs maintain optimum levels of network security and ensure that those logged in to the network are safe, and aren't opening up fellow classmates to the latest viruses?

In today's regulatory environment, it is essential for educational institutions to safeguard their confidential student and faculty data while keeping their networks accessible. Over the past ten years, a surge of compliance mandates including HIPAA, PCI, FERPA and others have



As new threats beyond simple worms and rate-based threats have emerged in recent years, Top Layer Security has kept up, evolving and enhancing its technology to help its customers face these new challenges.

created several requirements for stronger more effective information security, technology risk management, and internal control practices.

The security threats that these compliance mandates are intended to address are real and can have an immediate and adverse affect on educational institutions. For proper defense, an institution needs an ability to assess risk, protect against malicious code, detect and prevent intrusions to its network, monitor its security posture, and alert key personnel of such events that could affect the institution's stability.

Implementing a proper IPS solution is considered a “best-practice” for addressing security and availability concerns, and it is required under most information security and technology compliance mandates. Companies need to deploy the right IPS solution as a fundamental component of their IT security strategy. Once complete, they will be in a stronger posture for the next wave of audits and attacks, while lowering the cost of operation and delivering necessary information to help decision-makers achieve a “risk/reward” outcome.

A solid and secure network infrastructure helps academic institutions offer a quality education and a wealth of learning opportunities. Educational institutions must provide secure and reliable network services for students and staff while protecting the confidentiality of records and data. Safeguarding against the liability of cyber attacks launched internally, and reducing threats to student users, are key measures of success.

Combined with a defense-in-depth strategy, Top Layer's award-winning IPS 5500 intrusion prevention system allows academic institutions to:

- Protect school district IT departments from malicious threats and network attacks
- Maintain dependable network performance for all students and faculty
- Protect confidential information, such as student and faculty records
- Ensure a safe exchange of information between students, faculty, and outside affiliates
- Block specific P2P applications that significantly increase the risk of malware and copyright violations



The IPS 5500 is the first and only IPS solution as rated by NSS Labs that seamlessly integrates stateful firewall filters with multiple content-based and rate-based protection mechanisms on a single platform. Top Layer IPS solutions can therefore be deployed at the network perimeter or elsewhere on the network in front of servers that host critical applications and databases.

Leading educational institutions such as the University Of Miami Leonard M. Miller School of Medicine leverage the Top Layer IPS solution to meet the unique network security requirements all educational organizations face: providing highly-available and reliable network performance while providing both open access to students and dedicated protection of student data and proprietary research information. To download the full case study, please [click here](#).

As security threats evolve and become more cunning and sophisticated, educational institutions require security solutions that can address their complex and ever changing needs. The IPS 5500 is the only solution that can deliver the right protection, performance, and reliability to provide a secure and reliable network for students and staff.

***For more information on Top Layer Networks and its award winning IPS
Call +1 508-870-1300 x1 or visit our website at www.TopLayer.com***

About Top Layer

Top Layer is a leading provider of Network Intrusion Prevention Systems (IPS) that reduce organizations' risks and losses by protecting critical online assets against cyber threats. Its family of high performance IPS provides the most advanced protection against known and zero-day threats at maximum throughput rates. Top Layer is headquartered in Massachusetts, USA, with Global Sales and Support throughout North America, Europe, Asia, and Japan.

Rev 1.0 Mar-02 © 2009. Top Layer Networks, Inc. All Rights Reserved. Attack Mitigator, DCFD, Flow Mirror, IDS Balancer, TopInspect, TopMSS, SecureCommand+, and ProtectionCluster are trademarks of Top Layer. AppSafe, AppSwitch, SecureWatch, Top Layer, Top Layer Networks, TopFire, TopFlow, TopPath, TopView, and perfecting the art of network security are registered trademarks of Top Layer. Unless otherwise indicated, Top Layer trademarks are registered in the United States and may or may not be registered in other countries.

**Top
Layer™
Security**