

## MARKET BRIEF

# Helping to Protect the Open Campus

To fulfill their functions of educating students and promoting research, college and university campuses must be open to the flow of people and ideas. But at the same time, they should protect the physical safety of their students, faculty and staff as well as the integrity of their data and the information systems that handle that information.

Achieving a balance between these two needs requires flexible, highly configurable security tools that can be adapted to the unique needs of the higher education environment. It also requires skilled professionals who can strike the proper balance between security concerns and openness, and who understand the public safety concerns facing today's campuses.

### Physical Security

While campuses are generally safe environments, they are vulnerable to the same natural and man-made disasters as any other institution. In the event of such an emergency, the school administration needs to quickly identify and understand the situation; warn students, faculty and staff away from the affected area and account for their status, and coordinate the actions of its own first responders. While no campus can claim to be entirely safe, the presence of sound security practices and systems are essential to its continued smooth operation.

### Information Security

Colleges and universities run on information, much of it highly sensitive and damaging if stolen, made public or otherwise compromised. This includes student records such as transcripts, demographic data and admissions profiles; data generated by researchers; financial information about the university and about individual students as well as health information about students, faculty and staff.

However, implementing security in a campus environment is especially challenging because of the large number of users and the multiple ways in which they access the college network. Some may use conventional wired network connections, others may use WiFi links, some will connect from desktop or notebook computers while



still others may use PDAs, smart phones, or other handheld devices. Finally, there is the fact that college campuses have a large number of occasional users, including student guests as well as visiting faculty and staff. A school's chief information security officer has the challenge of allowing appropriate access for such individuals without allowing hackers to introduce malware into the network or to compromise sensitive information.

### How AT&T Can Help

AT&T products and services can help campuses prepare for, and cope with, natural or man-made disasters.

AT&T operates the largest wireless voice and data network in the country. These can be used both for disaster response planning and to provide reliable communications in the wake of an emergency.

AT&T provides a wide range of security services which provide a "defense in depth" approach against a wide range of network-borne attacks, allowing campus IT administrators to balance access with protection. These include:

AT&T's Managed Intrusion Detection Service remotely monitors the campus network for a continually-updated database of over 1000



existing attack signatures. When an attack is detected, the system automatically responds according to the school's predefined policies.

A range of firewall services to scan Web traffic for malware and other known threats. These firewalls may be located on the customer's premises, on the AT&T network or on endpoints for remote access users subscribing to AT&T Premises-Based VPN Service and AT&T Business Internet Service.

AT&T VPN services encrypt the data and thus helps protect sensitive data traveling over public data, voice and Wi-Fi networks. Its NetMotion solution even provides mobile VPNs for users on the move.

AT&T Internet Protect® security and alerting notification service offers advance information on known viruses, worms and DDOS attacks.

AT&T Intrusion Prevention Service helps detect, contain and neutralize known threats from hackers, viruses and worms attacking any IP-enabled endpoint on the client's network.

AT&T Secure E-mail gateway combines network-based spam filtering, virus protection, content management, email policy enforcement, message archiving and disaster recovery.

AT&T Managed Token Authentication Service protects critical systems by requiring users to have both a password and a physical token to access systems.

AT&T Web Security Service includes Web filtering, Web virus scanning, spyware screening and instant messaging control.

For campuses unsure of which security issues are most critical to address, AT&T can help them evaluate their current security posture and recommend remediation steps.

AT&T Consulting Services can provide security services ranging from creating a strategy and roadmap through architecture and integration to assessment and compliance.

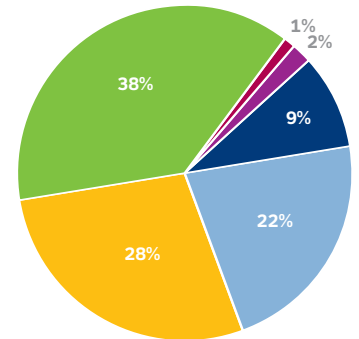
**Key Benefits**

**AT&T Security Solutions Help Campuses:**

- **Protect campus data through VPNs and token authentication**
- **Secure campus networks through firewall, intrusion prevention and detection, email gateways and more**
- **Find and address weaknesses in their security systems**

**Incident Breakdown By Type**

- Unauthorized disclosure
- Employee Fraud
- Impersonation
- Loss
- Penetration
- Theft



SOURCE: "Educational Security Incidents (ESI) Year In Review – 2007" Educational Security Incidents Research Project

**For more information contact your AT&T Representative or visit us at [www.att.com/edu](http://www.att.com/edu).**