



# Building a Comprehensive Solution for IT Security in Education

A tailored approach to multi-layer security

A Datamonitor white paper

Publication Date: April 2007

[www.datamonitor.com](http://www.datamonitor.com)

**Datamonitor USA**

245 Fifth Avenue  
4th Floor  
New York, NY 10016  
USA

t: +1 212 686 7400  
f: +1 212 686 2626  
e: [usinfo@datamonitor.com](mailto:usinfo@datamonitor.com)

**Datamonitor Europe**

Charles House  
108-110 Finchley Road  
London NW3 5JJ  
United Kingdom

t: +44 20 7675 7000  
f: +44 20 7675 7500  
e: [eurinfo@datamonitor.com](mailto:eurinfo@datamonitor.com)

**Datamonitor Germany**

Kastor & Pollux  
Platz der Einheit 1  
60327 Frankfurt  
Deutschland

t: +49 69 9750 3119  
f: +49 69 9750 3320  
e: [deinfo@datamonitor.com](mailto:deinfo@datamonitor.com)

**Datamonitor Asia Pacific**

Darling Park  
Tower 2, Level 21  
201 Sussex Street  
Sydney NSW 2000  
Australia

t: +61 2 9006 1526  
f: +61 2 9006 1559  
e: [apinfo@datamonitor.com](mailto:apinfo@datamonitor.com)

**Datamonitor Japan**

Wakamatsu Bldg 7F  
3-3-6 Nihonbashi-Honcho  
Chuo-ku  
Tokyo 103-0023  
Japan

t: +813 6202 7681  
f: +813 5778 7537  
e: [jpinfo@datamonitor.com](mailto:jpinfo@datamonitor.com)

#### **ABOUT DATAMONITOR**

Datamonitor plc is a premium business information company specializing in industry analysis.

We help our clients, 5000 of the world's leading companies, to address complex strategic issues.

Through our proprietary databases and wealth of expertise, we provide clients with unbiased expert analysis and in-depth forecasts for six industry sectors: Automotive, Consumer Markets, Energy, Financial Services, Healthcare, Technology.

Datamonitor maintains its headquarters in London and has regional offices in New York, Frankfurt and Hong Kong.

## INTRODUCTION

The lifeblood of education is the flow of ideas and information. The free and open exchange of ideas between students and educators is what allows those working in education institutions to transfer knowledge and understanding. However, providing and sustaining this environment of open ideas is too often easier said than done. External constituency groups, such as parents, taxpayers, policymakers and even the business community, all want to influence schools and pull them in often conflicting directions. Education is everyone's favorite tool for improving society or producing a wealthier country, but it also the favorite scapegoat for social problems or economic underperformance.

Information technology offers education institutions a powerful tool to realize their goals and hence help to mitigate the many pressures that they face. IT's function is to manage the flow of data and it has a vital role to play in the exchange of knowledge. Technology also has just as vital a role to play behind the scenes making school districts more effective and efficient in their administration.

However, IT is not immune from the pressures that school districts face. In addition, IT within education is open to the same security challenges that all other organizations face. These threats are often exaggerated by the special circumstances in which education institutions find themselves. In particular the fact that the primary users of IT within institutions are students rather than employees makes managing their computing very different to managing the IT for office workers.

In securing the computing infrastructure of education institutions, IT decision-makers – as elsewhere in education – need to carefully balance competing priorities. For example, they need to balance the need to preserve the safety and security of students and their computers with the desire to encourage freedom of enquiry. They also have to balance the natural desire to control the ways in which computers and other devices are used within the institution with the fact that students, and their parents to some degree, expect and demand increasingly unfettered access.

The IT security challenges for all education institutions are formidable. It is important to understand the roots of these problems before grappling with the potential solutions. In this white paper, Datamonitor will address the following questions:

- What pressures are education institutions facing and how do these pressures influence IT development?

- How do student preferences and sensibilities generate challenges for IT security?
- What strategies can institutions adopt to address formidable security challenges?
- What are the key factors institutions must consider in order to build a secure IT infrastructure?

## IT SECURITY IS A SIGNIFICANT CHALLENGE FOR EDUCATION

Education is beset by a range of conflicting demands from a diverse constituency. Schools are tasked with graduating both engaged citizens and productive workers, fostering a love of learning while drilling the students with hard facts. Further exacerbating these challenges is a political context where institutions are expected to provide better service at a lower cost.

The pressures placed on schools to both deliver social change and drive economic growth have never been greater. The insistence from parents that their children receive the best possible start in life means that institutions must often compete to win students.

IT can help education institutions to address their challenges. It can reduce the cost of administration, through student information systems (SIS) and other enterprise solutions to manage data more efficiently. More importantly it can help to both increase the effectiveness of the education itself and make education cost efficient, through solutions such as online learning.

However, IT can do none of these things if systems are not both stable and secure. The challenges faced by these institutions can mean that they can often be poorly placed to take advantage of the solutions that IT has to offer. Specifically education faces particular challenges in implementing IT solutions:

- **Size** – Many schools have difficulty justifying investment in the enterprise IT systems that they need because they lack sufficient scale to fully benefit from them.
- **Shortage of IT staff** – Institutions find it hard to afford sufficiently qualified staff to either implement new solutions or to maintain those they already

have. Smaller schools may not have any specialized IT staff at all and rely on teaching staff to manage the purchasing of IT.

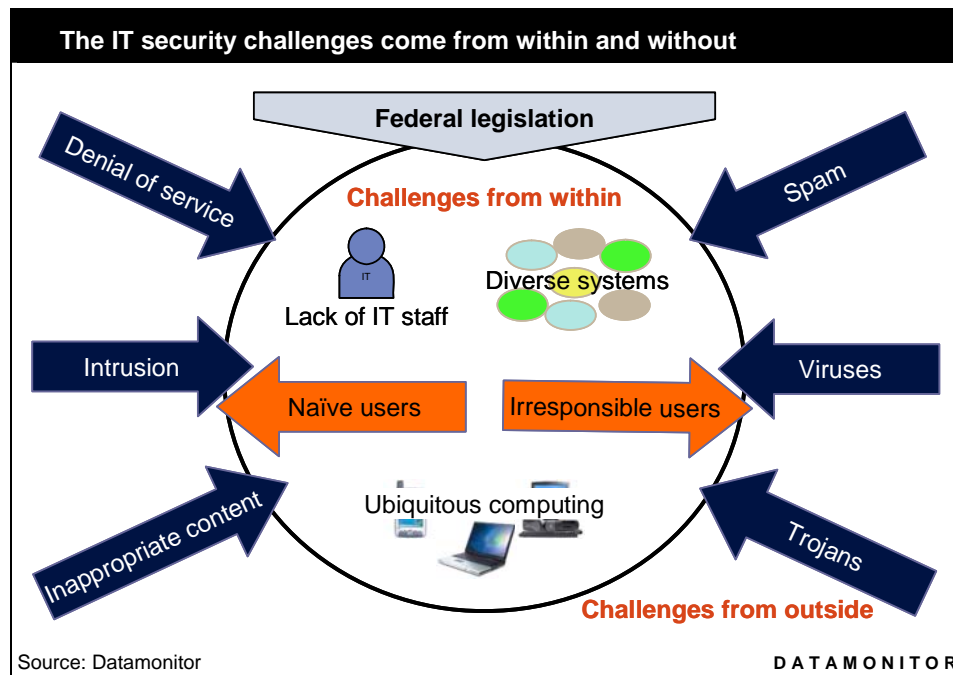
- **Insufficient budgets** – Small schools not only find it challenging to recruit and retain staff, but also to raise the capital funds necessary to invest in substantial IT projects. Even larger school districts find that the squeeze on budgets makes it hard to find the necessary resources for the technologies needed to provide education and secure the IT infrastructure itself.
- **IT funding is not flexible** – Much of the money available to schools and school districts is allocated for specific technologies, which do not always include those most needed. Specifically E-rate funding for telecommunications does not explicitly fund most IT security applications. School districts are left with the ability to fund connectivity, but not the extra security that should come with it. However, some more basic applications such as firewalls may receive funding and making use of Billed Entity Applicant Reimbursement (BEAR) can help to provide the cash flow for funding security spending.
- **Diverse technology** – While businesses can often impose uniformity on the technology in use in their organizations, education IT departments often have to deal with a wide variety of operating systems and devices. Even where the number of private machines is not large, education institutions often have a wide range of different legacy devices attached to their network. Upgrade cycles are slow and purchasing of PCs is often not under central control. Some schools will have PCs running almost every version of Microsoft Windows from 95 through XP SP2.

Paying for IT and for IT security in particular always represents a challenge for cash strapped school districts. In order to raise the money for necessary IT investments – especially to protect student and their IT systems – school districts should be prepared to think creatively about the sources of funding available to them. Making the best use of e-rate is obviously a good first step, but other alternative methods can also prove effective at providing the required funds, especially for capital investments. For example, when seeking finance for individual projects that entail high upfront cost, school districts can contemplate the use of a one off local sales tax – where eligible – which may be promoted to address a specific educational purpose. This single hypothecated tax can be particularly successful for popular schemes such as laptop purchasing or protection of young students online.

## Cyber security is a key IT driver for schools and school districts

Maintaining IT security is consistently a core concern and a key priority for people managing IT in any industry. The unique contextual pressures facing education institutions mean that if anything, this focus on security is even greater. In particular the need to support and yet protect young people's use of technology throws up a number of distinct challenges:

- **Behavior** – Students can't be relied upon to follow security policy, either because they are unaware of the policies or don't understand what is required;
- **Protection** – Content from outside the organization needs to be filtered to protect vulnerable users;
- **Legislation** – Parental concerns have resulted in federal legislation with which district must comply;
- **Ubiquitous computing** – An increasing number of school districts have one to one student to computer ratios and these machines all need to be kept secure.



## Behavior

It has become a cliché that the greatest threats to IT security are the result of human factors rather than IT weaknesses. The “human factor” is challenging with any set of users, but is much more so when those users are students.

Students are not employees. An employer can design a security policy and hold end users accountable for following that policy. Students, however, may be unwilling or unable to obey the security policy. Not only do students often see getting around the technologies designed to protect them and the IT systems as a challenge, they can also fail to understand the consequences of their behavior. Tell many students not to press the red button and their immediate reaction is to press it.

## Protection

Schools face the challenge of their moral and legal duty to protect their students. The Internet and email can bring a wide variety of unsuitable unsolicited material to children. Content filtering is often the main IT security priority for schools and school districts.

At the same time, the school will want to encourage students to make independent use of the Internet as a learning tool. Parents expect their children to acquire advanced IT skills which are impossible to develop without the freedom to use the Internet.

As the use of the Internet evolves, it presents both new opportunities for learning and poses new threats to students. In particular the rise of social networking sites – of which Myspace is by far the most famous – poses a particular challenge. Social networking can have educational benefits and enable students to form productive connections with their peers across the world. Schools need to find ways to make use of developments in online culture while at the same time still protecting students effectively.

## Legislation

Fear of the threats to children from the Internet has stimulated legislators to act to impose further restrictions on students’ IT use. The Children’s Internet Protection Act

(CIPA) requires that schools operate "a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are obscene, child pornography, or harmful to minors." Institutions which fail to comply risk the loss of e-rate funding.

The Deleting Online Predators Act (DOPA) which is currently before US legislators will, if passed into law, make schools responsible for placing very strong restrictions on what minors using computers should be allowed to do. The Act has drawn most of its publicity for its ban on the use of social networking sites, but it is the obligation to adapt to an ever changing Internet environment that will present the greatest challenge for schools districts. In its current form the act also obliges the institution to be able to turn off parts of the ban when a child is directly supervised, creating yet another technology challenge.

## Ubiquitous computing

The model for using IT in schools is changing from a segregated room with static IT desktops to model wirelessly networked devices that travel with the student or teacher. An increasing number of school districts are in the process of creating a situation where every student and educator has such a device for use at home and school. In a 2006 survey by America's Digital Schools, 24% of respondents said that their district was transitioning to a one to one model for computer usage.

The movement towards ubiquitous computing generates a number of fresh IT management challenges, resulting from the large number of new devices which need to be supported and provided with network access. In particular, securing these devices for use both at school and at home presents a particular difficulty. Students need to be provided with secure wireless access in the schoolroom, to have these individual machines secured against malware and potentially to have secure access to school systems from home. In addition, IT managers will want to control the applications installed on the devices offsite to ensure their smooth operation with school systems.

## Additional challenges

In addition to the concerns relating to the student IT user, institutions also face other difficulties that, while not unique to them, are more exaggerated in education than in other types of organization.

- **Student information confidentiality** – Institutions hold a wide variety of personal data and have a legal obligation under Family Educational Rights and Privacy Act (FERPA) to make sure that it is kept secure.
- **A heterogeneous environment** – The variety of machines and operating systems mentioned in the previous section creates particular problems for those trying to secure the network. Machines require different anti-virus software that has to be updated at different times and there is little prospect of keeping track of compliance on all machines.

The challenges facing the IT systems of education institutions may seem formidable. However, vendors have increasingly developed solutions that can help institutions to address these challenges.

## **A STRATEGY FOR MULTI-LAYER IT SECURITY**

Clearly education institutions face security challenges that fully justify the clear priority that decision-makers have given to solving them. However, the question remains how to use the plethora of solutions available in the market to address these issues. In this section Datamonitor will consider the options institutions have for addressing the challenges of IT security while meeting their own institutional needs. Datamonitor will also look specifically at the solutions offered by AT&T and how they fit into an overall security solution for a particular institution.

As in other areas of IT investment, when procuring IT security, it is vital to identify the right partners to work with, who can match their particular strengths to the unique problems facing the institution. In education, it is especially crucial that the partner is able to provide the right degree of advice and support to help already over-burdened IT departments. Honest and reliable advice in the procurement process can be far more important to institutions than additional features.

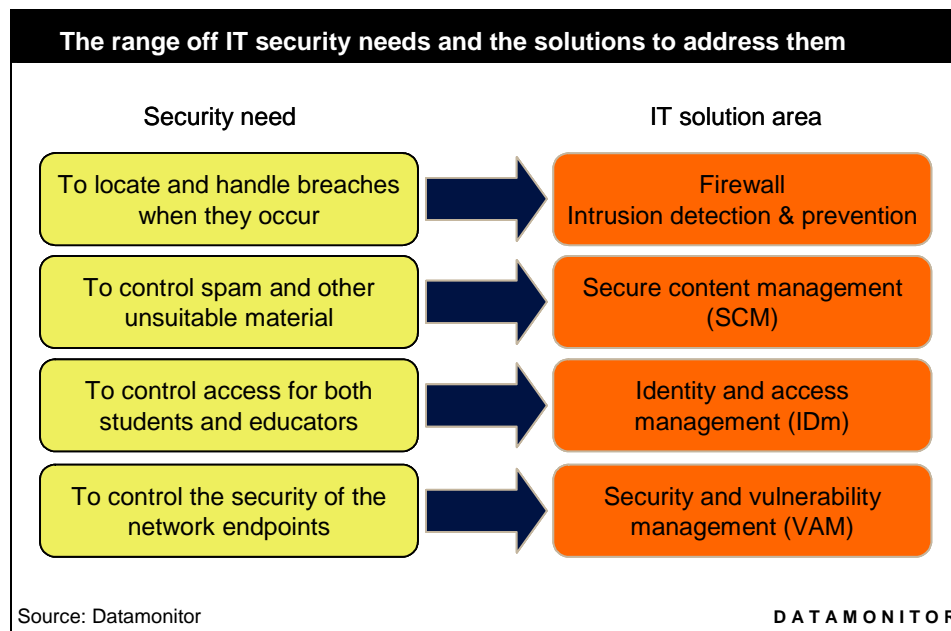
Any security solution must be flexible enough to meet student and teachers needs. A solution that requires too much of younger end users or their teachers will struggle as a result of an inconsistent or only partial implementation. Equally one which is so restrictive that it inhibits learning will end up being circumvented or may even have negative impact on institutional effectiveness.

One way to provide flexibility in the IT security architecture is to make use of separate defenses for separate systems. For example, making use of individual firewalls around particular systems – perhaps those that contain personal data – within the

main firewall gives those systems an additional layer of protection. Sensitive data can be protected more thoroughly without unduly restricting other users on the network. This defense in depth strategy offers greater security for the systems as a whole by increasing the number of hurdles that a hacker or virus has to jump over. By using different types of solution along side each other security can only be enhanced.

To address both the need for flexibility and the need for extensive support, institutions can turn to some form of managed service. This does not mean outsourcing all of an institution's IT security systems security – although this may be possible. Instead security services provided by a network operator can act as part of a larger solution, by adding extra layers to the proverbial security onion.

Like other organizations, the IT security needs of education institutions can be broken down in several different areas each with its own corresponding technology solution area, as shown in the diagram below.



In general, education institutions should consider using hosted security solutions—such as those offered by AT&T – as part of their overall security architecture. Hosted solutions offer ways around some of the key challenges faced by education institutions:

- **Overstretch** – For IT departments who lack the personnel to adequately support a wide array or complex set of security solutions, a hosted solution offers a compelling option. Maintaining the solution is no longer a problem for the under-equipped internal staff.
- **Capital spending** – When institutions lack the budget for capital investment in large IT solutions, moving security to an operational or recurrent expense becomes an attractive strategy. When the cost of maintaining and installing systems are taken into account hosting is often more cost effective overall, as well as fitting better with cash flow needs.
- **Scale** – Hosted solutions give smaller institutions access to the kinds of robust IT security solutions used in large enterprises. These solutions offer better protection against security threats than the smaller premise based solutions that small institutions can support themselves.
- **Flexibility** – A hosted provider should be able to provide the kind of flexibility to deal with changing need with the organization having to rip out and replace onsite solutions. For example, if the institution grows very rapidly it doesn't need to replace the small scale systems it had with an enterprise system as the hosting provider already offers access to this kind of system.
- **Experience** – One of the most valuable things that a large hosting provider such as AT&T is able to provide is considerable experience and expertise in a variety of different systems and their problems. As a result, they will have been involved in developing solutions for education institutions that have given them experience that can be applied directly to other institutions.

## Firewall and intrusion prevention

Firewalls have been the traditional first line of defenses for any organization's IT systems. While newer security solutions have emerged, firewalls should remain a core part of an institution's IT strategy for two main reasons:

- **Reliability of the perimeter defenses** – Firewalls are a tried and tested solution which can be relied upon to do exactly what they claim to do. While a firewall may be no defense against the more sophisticated attacks or more outrageous examples of end user behavior they are still a vital first line of defense for all organizations.

- **Building defense in depth** – As well as reinforcing the edge of the network, education institutions, particularly those with multiple systems, can choose to defend in depth. This means placing firewalls around individual systems that lie within the primary firewall, so that attacks have to penetrate two layers of defense to reach these systems. To pursue this strategy, institutions can augment a general firewall with individual appliance based firewalls to sit next to these internal secured zones.

Networked based firewalls, such as that offered by AT&T, offer institutions the option of moving the first line of defense to the network provider. A firewall hosted on the network might provide all the cover that the institution needs or as mentioned above may free valuable internal IT staff to secure individual systems using smaller firewall solutions. In addition, a network based firewall makes it easier for the IT department to cover multiple locations without separate solutions and gives smaller institutions access to a constantly updated enterprise-class firewall.

Intrusion detection and prevention can be seen as the natural second line of defense behind a firewall solution. These solutions enable the institution to take a deeper look at the behavior of users who have accessed the network and then can take appropriate action. By spotting the patterns of network traffic that indicate trouble the solution can then nip this rogue activity in the bud.

Intrusion detection and prevention solutions can be based locally or hosted. Again hosted solutions, such as that offered by AT&T, can offer significant advantages to overstretched and under funded IT departments in education. Recognizing the signatures of rogue behavior requires that the database of these signatures is sophisticated and constantly updated, both functions that a large hosted provider is in a position to provide.

In addition to these standard hosted solutions AT&T is able to provide its Internet Protect<sup>®</sup> solution, which makes use of AT&T's unique access to information and activity on AT&T's Global IP backbone. AT&T has possibly the largest IP backbone in the world and its Internet Protect solution makes use of this information in order to prepare its customers against emerging threats. Many worms and viruses can be identified well in advance of becoming a significant threat to institutions. Internet Protect customers get access to a web portal that shows Internet traffic and identifies any anomalies that they should be watching while also providing mitigation recommendations.

## **Secure content management**

Secure content management is made up of anti-virus, content filtering and web filtering solutions.

Schools are increasingly obliged to shield their students from unsuitable content both from email and the web. As this obligation expands, preventing spam email is not just a matter of keeping out viruses, but of ensuring that all manner of inappropriate content is successfully screened. Web and email content filtering is probably the biggest source of pressure on IT managers in school districts, thanks to growing parental and political concern.

AT&T Web Security is a hosted network-based service which can provide controlled Internet access for a school's web page requests, web content and instant messenger (IM) exchanges. As well as watching for viruses and other malware, the system is able to offer web filtering and control over the IM applications that the school may allow students to use. Protection from viruses and spyware is very important in an environment where naïve young users may unwittingly attempt to download damaging programs. However, it is the ability to manage students' access to content that can provide the greatest value to school districts.

By opting for hosted web filtering, the school district can benefit from the constant updates to the systems, as the provider learns from collected user experiences. The AT&T Web Security solution offers the ability to both manage the solution through a web portal and receive reports on usage, to provide evidence of compliance.

In addition, AT&T offers a hosted email application that also provides email filtering and spam control. By opting for a completely outsourced email application, institutions gain access to the scalability of a network provider email system, as well as security systems that are updated more regularly than is practical in a premise based system.

## **Security and vulnerability management**

Security and vulnerability management technologies include those that monitor secure computers attached to the network. Vulnerability management and patch management solutions offer a way for institutions to test systems for known vulnerabilities and to apply patches where appropriate. Although these systems offer an excellent way to help institutions cope with the wide variety of machines connected to their network, they are often viewed as too large and expensive to implement, particularly for smaller institutions.

However, by moving to a hosted solution – such as AT&T's Endpoint Security product – institutions can gain this greater control over their network endpoints without the need to find the budget for a large scale premise based solution. The solution installs software on the laptop or desktop PC being connected to the network. As soon as the PC is turned on it is checked against the policies for accessing the network. If the device does not comply with the policies then the network does not let it log onto the system. If the policies change on the network, this is pushed to all of the devices that try to connect with it.

## PRACTICAL RECOMMENDATIONS FOR IT SECURITY

Education institutions face significant business and IT challenge, but by making use of the right security technologies institutions can overcome these challenges and provide better services to their students, faculty and staff. In constructing the right security architecture for your institution, Datamonitor makes the following recommendations:

- **Clear assessment of need** – Understanding your own IT security needs is vital before trying to address them. To do this it is important to identify the goals of your security solution and to have an honest assessment of the current state of your systems.
- **A multi-layered approach** – Defense in depth can provide both greater security and greater flexibility. No one security product offers complete protection against IT security threats. Several solutions of the same type, such as multiple firewalls, can give you the ability to adapt to the contrasting security needs of different stakeholders, while decreasing your overall exposure to threats.
- **Hosted solutions** – Hosted solutions offer significant potential advantages for education institutions. For smaller intuitions in particular, a provider of hosted security technology can enable you to take advantage of large scale solutions at a cost effective price. Hosting part of the security solution can also form an important part of a strategy of defense in depth for larger intuitions whose existing defenses need to be strengthened.
- **The right partner** – The right partner should have a clear track record in securing institutions like your own. It is important that in considering partners your intuition moves beyond a check list of features and simple price comparison. Finding the right solution provider is not just about finding the

right technologies it also about finding the right advice and support in this most complex of technology decisions.