



# 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 not only to transfer knowledge and understanding, but to develop and improve it as well. 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 education institutions and pull them in often conflicting directions. Education is everyone's favorite tool for improving society or producing a wealthier country, but it is 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 both the exchange and the discovery of knowledge. Technology also has just as vital a role to play behind the scenes making educational bodies more effective and efficient in their administration.

However, IT is not immune from the pressures that education institutions face. In addition, IT within education is open to the same security challenges that 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 from 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. Consider that institutions 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 lower cost.

The pressures placed on education have never been more acute thanks to the increasing competition that institutions face for students. Higher education institutions face a challenging demographic situation at home. In addition, as other English speaking nations such as the UK and Australia seek to expand their recruitment efforts internationally, the market for international students – traditionally viewed as a source for new students – has never been more competitive.

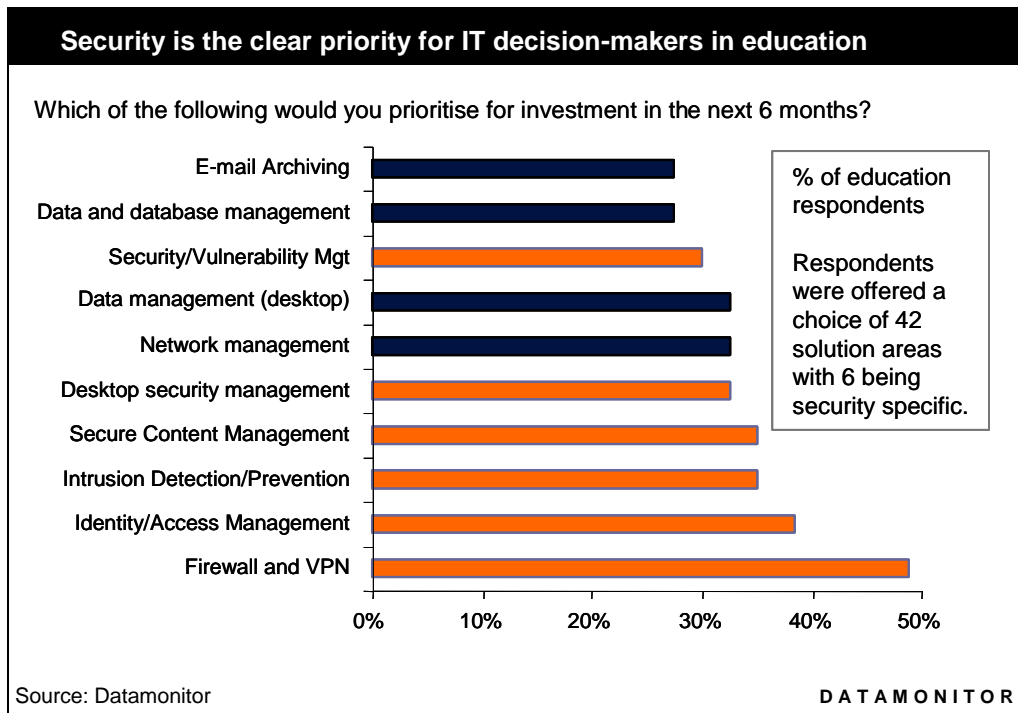
IT can help education institutions address their challenges. It can reduce the cost of administration, through student information systems (SIS) and other enterprise solutions to manage data more efficiently. It can help with student recruitment through customer relationship management (CRM). More importantly it can help to both increase the effectiveness of the education itself and make education cost efficient, through its application to the learning environment.

However, IT can do none of these things if systems are not both stable and secure. As a result of unique contextual challenges, institutions are often poorly placed to take advantage of the solutions that IT has to offer. Specifically education faces particular challenges in implementing IT solutions:

- **Size** – Many colleges 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 colleges find it particularly challenging to recruit qualified staff, given the relatively low salaries they are able to pay.
- **Lack of money** – Small colleges not only find it difficult to recruit and retain staff, but also to raise the capital funds necessary to invest in substantial IT projects. Even larger institutions find that the squeeze on budgets makes it hard to find the necessary resources for the technologies needed both to provide education and secure the IT infrastructure itself.
- **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.

### **Cyber security is the primary IT driver for institutions at all levels**

The unique situation of education means that the IT departments of education institutions face a range of demands on their time and resources. However, when asked to prioritize different technology investments, security is the clear winner. The diagram below shows some results from Datamonitor's most recent *Technology Trends* survey. In this question, technology decision-makers were asked to pick from 42 distinct technology areas that they might invest in over the next six months. In responding to this question, educators chose security solutions more often than any other type of solution. In fact, all of the top five technology areas were security solutions and all of the security solutions which were offered as choices to respondents came in the top ten.



Without question, security is the overwhelming IT priority for education institutions, not just in the United States but across the western world. The primacy of security as a concern is a result not only of the general problems of IT security – which are keenly felt in all commercial and non-commercial enterprises – but also of the unique nature of computing users in education.

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.

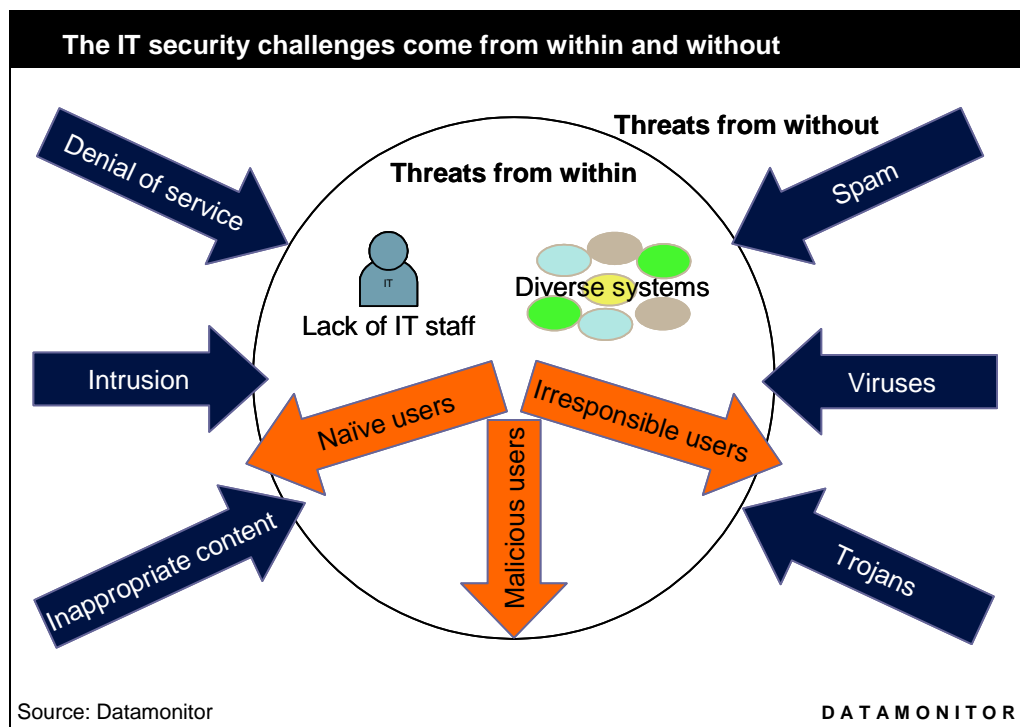
Students are not employees. An employer can design a security policy and hold end users accountable for following that policy. Furthermore, in most cases, the employer will also own and exercise control over the computers or other devices that form endpoints of the network. Students, however, often own their own computers. Even where the computers belong to the university, they may have been purchased from individual departmental budgets and are not under the control of the central IT department. Students may be unwilling or unable to obey the security policy and given they are clients of a service that the institution provides it can prove hard to insist.

Higher education institutions are a particularly open environment, where it is considered neither acceptable nor desirable to place strong restrictions on IT usage. Freedom to use IT resources in an open way is not only desirable as a matter of principle, it enables the innovative use of resources for both learning and research.

At the same time the institution has an obligation to look after its students. Students and their parents expect the school to protect them from malicious threats and to protect their devices from damage.

Higher education institutions must also take account of more directly malicious behaviors from within their own user base. Often they face a large group of well educated highly skilled individuals with time on their hands and sometimes a strong motivation to hack systems. Even if the students of a particular body are not attacking their own institution they may attempt to use its resources to attack other targets. A significant number of purely vandalism viruses originate amongst students.

As a result, as illustrated below, for educational institutions IT threats come from both outside the institution and from inside.



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.

- **Mobility and wireless** – Wireless networks and the desire to deliver content on mobile devices such as smart phones generate significant security challenges.
- **Hijacking by hackers** – The considerable IT resources behind a university's firewall can make a tempting target for hackers mounting denial of service attacks.
- **Personal information confidentiality** – Institutions hold a wide variety of personal data and a number of high profile incidents of data being compromised have focused attention on lax security in some institutions. Ohio University witnessed the theft of Social Security numbers and other personal information on more than 173,000 alumni, students, staff and others. This incident led the university to invest \$4 million in an effort to secure their systems against future attacks. Information leakage scandals of this type can have an adverse affect on both recruitment and alumni fundraising, so preventing them is a priority for Higher education institutions in a competitive market.
- **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 on 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.

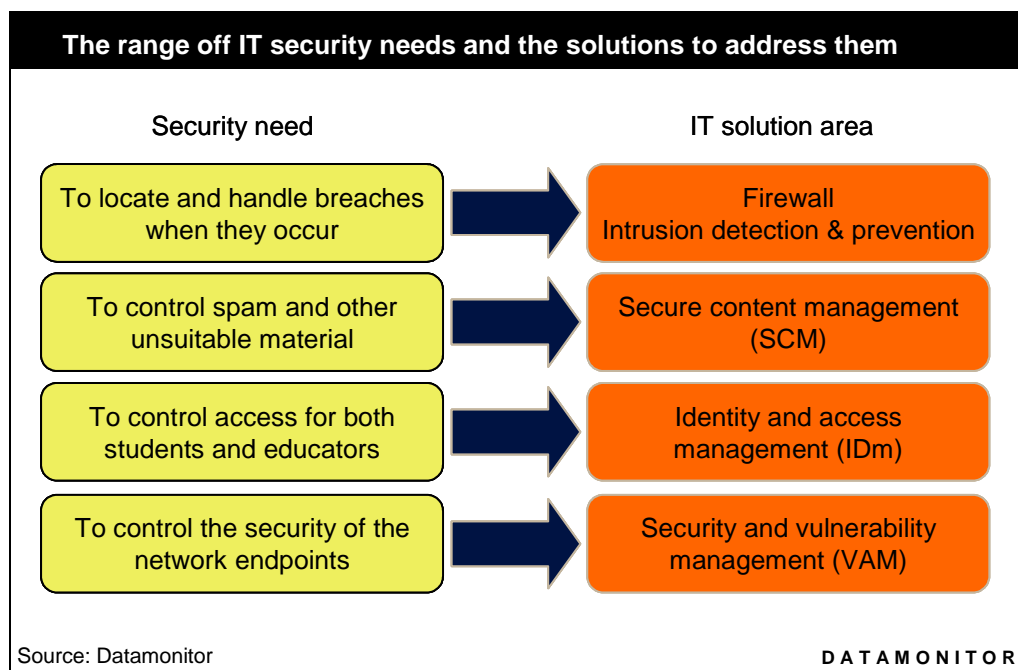
As in other areas of IT investment, when procuring IT security, it is vital to identify the right partners to work with, who can match their particular strengths to the unique problems facing the institution. In education, it is especially crucial that the partner is able to provide the right degree 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.

Given the fact that many of the challenges faced by education IT departments are the result of the behavior of student users it is vital that any security solution is flexible enough to meet student needs. A solution that requires students to behave in a way that doesn't fit with their computing use or is seen to restrain academic freedom will fail thanks to lack of compliance.

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 intuitions 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 the changing needs of the organization without

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 intuitions 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 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 rouge 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 rouge 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.

Internet Protect also incorporates an option to provide extra protection against distributed denial of service (DDOS) attacks. The DDOS Defense is able to watch for and respond to attacks from multiple locations. For large institutions who may offer a tempting target to organized hackers this can be particularly valuable.

## **Secure content management**

Secure content management is made up of anti-virus, content filtering and web filtering solutions. Content filtering, in certain circumstances, may be interpreted as restricting traditional academic freedom. However, email spam is key source of viruses and while some may object to excessive filtering, students do want to be protected from drowning in an ocean of spam.

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.

## **Identity and access management**

Identity and access management (IDm) technologies include those that provide strong authentication, access controls and provisioning. IDm is particularly important to larger education institutions that have to handle access to their systems by a large and constantly changing student body and academic staff. Often these students and staff will want access to internal systems from offsite and all will have different levels of access privileges.

AT&T offers a token authentication solution, which provides students and staff with a unique pin and token that displays a constantly changing password for logging into the network. This prevents users from sharing passwords and control levels of access much more effectively. It also makes it easier to deal with the high turnover of student and staff.

## **Security and vulnerability management**

Security and vulnerability management technologies include those that monitor how secure computers attached to the network are. 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 the Endpoint Security product offered by AT&T – 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 set out what the goals of your security solution are and to have an honest assessment of what the current state of your systems are.
- **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.