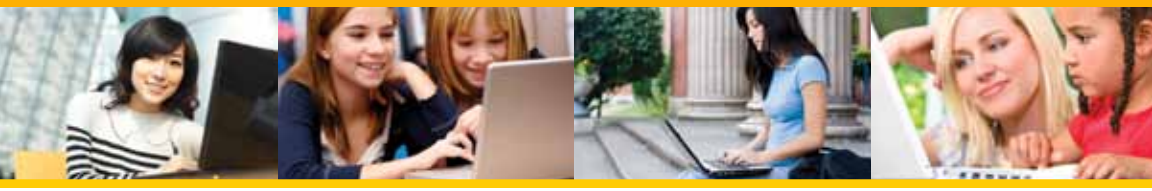

E-LEARNING
HANDBOOK

Practical strategies for secure online interaction among students, educators, administrators and parents

- Evolving forms of online learning
- Controlling network access
- Guarding against malware
- Mitigating compliance risk

Produced by CENTER FOR DIGITAL EDUCATION

For additional copies or to download this document, please visit:
www.convergemag.com/e-learning

E-LEARNING
HANDBOOK

Table of Contents

Finding a Way Forward

Online learning and digital interaction is pervasive in today's educational environment. Where rich multimedia content once was an exception, it's increasingly the rule in K-12 and college classrooms. Blended or hybrid courses that mix elements of traditional classroom learning with online education are the norm in many school districts and universities. And completely online courses — not to mention entirely virtual colleges and school districts — are emerging with growing frequency.

But educational institutions aren't just delivering learning content differently; they're interacting digitally with the diverse stakeholders that make up the education community. For instance, students access grades and transcripts online. Parents monitor student attendance electronically and e-mail teachers with their concerns. Students and teachers collaborate via social networks. School staff members conduct common employee transactions — choosing benefits, booking vacation time, etc. — through district Web portals. And the list goes on.

Yet, the vast potential of online learning and digital interaction comes with significant technology challenges. Broadening learning opportunities through multimedia tools, offering remote access to educational content, and letting users remotely tap into school data and systems demands that schools manage new levels of IT complexity and adopt more sophisticated approaches to IT security. This guidebook is designed to help educational institutions deal with these issues.

We'll examine significant trends in online learning to gain an understanding of what colleges and school districts need to prepare for. It's clear that technology is changing teaching models — both inside and outside of the traditional classroom. Funding reductions for public universities are forcing higher education institutions to reconsider the delivery model for college courses. Governors and mayors pressure school districts to improve student performance — especially in critical subjects like science and math. Educators and administrators search for effective — and affordable — approaches for keeping at-risk students in school and helping special-needs students succeed. Online learning and new forms of digital interaction play a growing and evolving role in all these issues.

But if technology is going to answer these challenges, the IT environment must be simplified. Therefore, we'll present strategies for managing growing technological complexity. Students, parents, teachers and administrators expect 24/7 access to course material, grades, attendance, admissions and more. What's more, they want to access that information from a dizzying array of devices, from traditional desktops and laptops, to smartphones and slick new tablets. Some of those devices may be owned and managed by the educational institution — but a growing number of them are not. How do you respond to all of this without deploying hundreds of conflicting applications and hiring an army of expensive IT professionals to keep it all straight? We'll show you some solutions through powerful technologies like endpoint virtualization.

Just as important, as schools expand the amount of online education and information they offer, how do they protect vital systems and data? A thoughtful approach to network and information security is absolutely fundamental to your success. Ten years ago, few students or parents regularly accessed school networks. Today, nearly every student — along with guardians, teachers and staff members — regularly accesses network resources. How do you keep this array of new users from introducing malware and viruses into critical school IT systems? How do you ensure that users only access data they're authorized to see? How do you stop them from inappropriately sharing private information or proprietary course material? We'll explain how solutions like network access control and data leak protection equip schools to address these concerns.

Finally, we'll examine key regulatory issues that impact online learning. Federal laws like the Health Insurance Portability and Accountability Act (HIPAA) and The Family Educational Rights and Privacy Act (FERPA) require protection of student medical and educational records and in some cases, carry significant liability for inappropriate release of that information. A rash of recent incidents where students used popular online social networks to attack other students is driving another legal trend: A growing number of states have passed laws against "cyber-bullying" to address the situation. We'll point out some of the rules you need to keep in mind.

It's clear that a confluence of factors is forcing changes to traditional K-12 and higher-education models. Students expect to use interactive and collaborative technologies to learn — just as they use these technologies to collaborate and socialize in their daily lives. Teachers, school districts, colleges and universities are under pressure to deliver better results and efficiency. Parents want value for their education dollar and meaningful access to academic information about their kids. These and other demands point to continued growth and innovation for online education. Educational institutions can't stand still. The ideas and concepts presented in this guidebook are designed to help you move forward.

Online Learning Trends

Technology continues to change education, but how? Identifying significant trends in online learning is crucial to understanding current needs, and it lays a vital foundation for future planning and preparation.

ONLINE MEETS THE CLASSROOM

Over the past five years, online learning has become integrated with traditional classroom learning to form hybrid or blended courses. These courses take different forms based on grade level, but they're designed to incorporate the best of traditional and virtual classes to deliver a better learning experience to students.

For instance, one Midwestern community college uses a blended model to meet the needs of students who juggle school work with job and family responsibilities. Students in the school's emergency medical technician program access lectures, take exams and participate in threaded discussions online. They also spend five Saturdays on campus practicing hands-on skills.

In higher education, arrangements like this are growing in popularity. Most respondents in the Center for Digital Education's 2010 survey of community colleges said between 35 and 65 percent of their students are registered for online or blended courses. In addition, colleges are providing multimedia lessons to students who download them for viewing and listening at their convenience. Full lectures can be recorded and viewed on a portable device whenever the student desires, replacing the traditional lecture hall. In-class time is devoted to discussion of the material and interaction between students and teacher.

A similar survey of K-12 school districts found that nearly 70 percent of respondents use video-conferencing technology for virtual field trips. Video presentations are routinely piped through school networks and delivered to classroom computers. High school history and science teachers also are pushing podcasts and video content to students as they prepare for exams.

"The use of online learning is becoming broader and broader — and it's increasingly integrated with traditional classroom learning," says John Halpin, vice president for the Center for Digital Education (CDE). "We expect these trends to continue as educators seek to improve student outcomes and make efficient use of school facilities, and as students demand interesting, interactive and portable course material."

THE RISE OF VIRTUAL SCHOOLS

It's also growing more common for students to enroll in online classes and attend completely virtual schools. In 2008, Florida lawmakers created the School District Virtual Instruction Program, which requires school districts to offer a virtual instruction program for K-12 students. Florida also is home to one of the nation's first Internet-based public high schools, the Florida Virtual School (FLVS), launched as a pilot in 1997.

FLVS is a fully accredited public virtual school that offers free online courses to middle and high school students in Florida. State officials say the school helps ease classroom overcrowding and gives students access to specific courses that may not be offered locally. FLVS also serves students who have medical or behavioral issues that limit success in the traditional classroom or for students needing flexible schedules due to training for other extracurricular endeavors.

The North Carolina Virtual Public School is another example where high school and middle school students can take accelerated courses, find classes not offered in local schools or keep up with studies while sick or injured. Most states offer some type of online public school courses to resident students. Some states offer full online high school diploma programs, while others offer a limited number of virtual courses. Florida and Idaho recently announced mandatory online courses for all high school students.

A study released in 2009 by the Sloan Consortium and Babson College researchers found that more than 1 million K-12 students were engaged in online courses nationally. Three-quarters of school districts responding to the survey offered online or blended courses, and 70 percent had at least one student enrolled in a fully online course.

Online learning numbers are even larger for higher education. In all, more than 5.6 million students were taking at least one online course in the fall 2009 term, according to another Sloan/Babson survey released in 2010. That survey of more than 2,500 colleges and universities found that 63 percent of reporting institutions consider online learning a critical part of their long-term strategy. Furthermore, the number of students taking online courses grew by nearly 1 million from the previous year, a 21 percent growth rate. Nearly 30 percent of higher education students now take at least one course online, the survey found.

A report by Ambient Insight, *The U.S. Market for Self-paced eLearning Products and Services: 2010-2015 Forecast and Analysis*, predicts a five-year compound decline of 22.08 percent per year in students attending traditional classrooms exclusively. The report

also states that by 2015, 25 million post-secondary students in the U.S. will be taking classes online. By that time, the number of students taking only online courses will be about equal to the number of students taking classes solely on a physical campus. The report predicts that if the trend continues, by 2018 there will be more full-time online students than students who take all their classes in a physical classroom.

"Clearly schools, colleges and universities will need to meet growing demand for online courses and blended-learning opportunities with competency-based practices, and they'll face increasing pressure to deliver rich, reliable, relevant and secure digital resources on mobile computing devices," says Sharnell Jackson, former e-learning Chief for Chicago Public Schools and now a senior fellow at the CDE.

TEXTBOOKS GO DIGITAL

Traditional textbooks are being displaced by electronic information, as educators and policymakers seek alternatives to expensive and quickly outdated hardcopy learning materials. For instance, former California Gov. Arnold Schwarzenegger launched the California Digital Textbooks Initiative in 2009, which will provide schools with a state-approved list of digital textbooks, starting with math and science. Schwarzenegger said the six-year replacement cycle for printed textbooks is simply too slow to keep up with rapid advances in technology, medical science and other fields. He added that shifting all of California's 2 million high school students to digital textbooks could save schools on the order of $400 million annually.

K-12 Technology

How online learning is used in elementary and high schools.

84% use Web 2.0 tools
88% offer online course credits
69% use video conferencing for virtual field trips

SOURCE: 2010 DIGITAL SCHOOL DISTRICTS SURVEY

Similar initiatives are taking root around the country. Virginia's Department of Education developed an online physics "Flexbook" designed to give teachers and students access to up-to-date lessons and techniques. The free resource, released in 2009, was authored by 13 K-12 physics teacher volunteers, as well as industry and university faculty.

The move away from physical textbooks means, by necessity, there will be more bandwidth pressure on educational networks to deliver digital content. There also will be more computing devices in students' hands. Some even predict that digital material — perhaps delivered on low-cost tablets or netbooks — could largely supplant traditional textbooks within the next five years. That timeline may prove optimistic, but the time to plan for such an evolution is now.

PREDICTING STUDENT SUCCESS

Schools are beginning to use predictive technology to keep kids on track, and use of these tools will continue to grow. This year, for example, Arizona State University will use adaptive learning software to deliver personalized instruction to math students. The software, which

will be tested in several classes this spring, lets students move through a course at their own pace and is designed to shore up weaknesses in their math foundation. The system tracks how students learn and serves up a combination of material designed to get them through the course as efficiently and effectively as possible.

Some of these predictive systems also are designed to send recommendations and reminders to students. Therefore, a student may receive a phone or e-mail warning that they're projected to receive a low grade, along with recommended actions for bringing the grade up. These technologies also further the notion of putting the student at the center of the learning environment.

These systems currently are more common at private universities, but look for them to make their way into public universities and school districts as educators attempt to boost college graduation levels and high school retention rates. Predictive technologies also could increasingly work hand-in-hand with virtual courses designed to provide education alternatives for at-risk students and other special-needs populations.

Community Colleges: What's Online

Here are the services community colleges offer to Web and mobile device users.

Course Management	**100%**
Mobile Interface	**22%**
Electronic Payment	**94%**
Mobile Interface	**15%**
Grades	**99%**
Mobile Interface	**20%**
Transcripts	**71%**
Mobile Interface	**16%**
Video/Audio on Demand	**57%**
Mobile Interface	**14%**

SOURCE: 2010 DIGITAL COMMUNITY COLLEGES SURVEY

MORE USERS AND MORE MOBILITY

Finally, educational institutions at all levels face explosive growth in the number of users accessing their networks. Teachers, parents, students, administrators, staff members and others routinely tap into school information systems. What's more, a few years ago, most users may have reached your network through a wired connection and a desktop PC. But today, they're likely to be accessing that data using a smartphone or a Wi-Fi enabled tablet.

Almost all community colleges now offer online access to student grades, and 20 percent of them can deliver grades via a mobile application, according to the 2010 Center for Digital Education survey. Almost three-quarters provide online access to transcripts, and 16 percent offer a mobile app.

These numbers will grow as stakeholders in the educational community demand more — and more convenient — access to course materials, student records, performance data, employment resources and other information. Administrators and IT professionals must be prepared to deliver access to these resources securely and reliably.

Secure Online Learning

The success of online learning hinges on security. Schools hope to broaden learning opportunities by offering multimedia educational content, 24/7 access to online courses and student resources, and the ability to connect to school data and systems remotely. But meeting these goals requires a thoughtful approach to safeguarding data and information systems. This section provides an overview of necessary security strategies and tools.

NETWORK ACCESS CONTROL

The number of users accessing school networks — once a select few — has grown exponentially over the past decade. Thanks to a shift toward online access and transparency, that user group now includes students, teachers, parents, administrators and staff members. Schools routinely offer grades, transcripts, attendance and other student information online. Teachers and school staff also routinely interact with their employers online, carrying out a growing number of remote, electronic transactions. And as transparency and reporting requirements grow, administrators and policymakers may be tapping into an array of school data streams.

All of this points to the need for strong access control policies and technologies. "As schools provide greater access to more types of users, this can create a very complex security environment — it's much more difficult than for a typical business environment," says the CDE's Halpin. "Educational institutions will need sophisticated tools in order to safely allow more access to network resources."

Schools must have identity management solutions and password policies that ensure only authorized users gain access to network resources. They also need network access control that's effective and comprehensive. The network access control process consists of four steps:

- ***Discover and evaluate endpoints —*** This process should occur as endpoints, or users, connect to the network and before they access any resources. The security system needs to evaluate new devices attempting to connect to the network to ensure they meet minimum standards set by school IT policies. Organizations must check for anti-virus, anti-spyware and installed patches before granting network access. The system also should examine registry entries, running processes and file attributes for suspicious activity.

- ***Provision network access —*** Full network access should only be granted to devices with the proper security posture. Devices that don't comply with the school's minimum security requirements should be quarantined with little or no network access.

- ***Remediate noncompliant endpoints —*** When a device fails to meet minimum security standards, it needs to be brought into compliance before gaining network access. This is

particularly important in school environments where students may be using personally owned devices to access course materials, grades and other resources. Remediation processes can be designed to automatically install necessary security software and fix problems, or students can be directed to a remediation area to manually download the resources they need.

- ***Proactively monitor compliance —*** Security systems need to monitor end-user devices continuously, so that any change can be discovered and addressed immediately. A change in security compliance can happen at any time and can spell disaster if not discovered instantly.

MESSAGING SECURITY

Like other large organizations, schools and universities depend heavily on e-mail. It's often the backbone of communication among teachers, between teachers and parents, and between citizens and school boards. E-mail's pervasiveness makes it a primary target for virus writers, hackers, scammers and others. Instant messaging and Web collaboration also are extremely popular in educational environments for supporting classroom and online learning functions, as well as for socializing among students.

Schools and universities should deploy solutions that block and filter malware from e-mail and IM with a single application. These solutions should provide real-time monitoring and reporting for messaging traffic, as well as spam filtering. To protect sensitive student and employee data, schools also should consider content controls that prevent Social Security numbers and other personal information from leaving the network via messaging applications.

IP reputational analysis can be used to help determine whether the source on an e-mail is good or bad. If a particular IP address has a known history of distributing spam or viruses, connection attempts from that address can be rejected and e-mail and IMs can be blocked.

The most effective messaging security techniques use security tools at multiple levels throughout the network, with most filtering occurring as far out on the network edges as possible. Security should occur at every point in the network, from endpoints, to gateways, to messaging servers.

MOBILE SECURITY

Students, teachers, parents and school staff members carry a growing number of mobile devices — from traditional laptops to the hottest new smartphones and tablets. With the proliferation of wireless networks on campuses, these devices put information and collaborative applications at users' fingertips no matter where they are. But these devices also can expose the entire organization to data security threats.

Thanks to advances in technology, portable and even palm-size devices pack significant computing power and storage capacity. And through VPN technology, they can access crucial network data — health records, Social Security numbers, financial information, etc. — just as easily as wired desktop devices. These devices are a growing target for hackers, and because some of them — like high-powered smartphones — are relatively new, their security processes may be relatively immature. Here's some advice for shoring up mobile safety:

- ***Act now —*** The number of mobile endpoints is growing rapidly. Educational institutions must address security issues around mobile devices, especially smartphones and tablets, as soon as possible.

- ***Expand your definition of endpoints —*** Ensure that your standard information security policies include mobile devices — especially emerging high-powered handheld devices.

- ***Treat mobile devices as regular endpoints —*** New classes of mobile devices should get as much security attention as traditional network endpoints such as laptops and desktops.

- ***Consider mobile device management (MDM) solutions —*** MDM software is designed to secure, monitor and manage mobile devices. It can distribute applications and configuration settings to tablets, smartphones, laptops and other portable computers. It can also wipe data and applications from devices that have been lost or stolen.

DATA LOSS PREVENTION

Preventing data loss is a key consideration for schools and universities. Educational institutions are required by various state and federal regulations to protect student identities, health information and other data. Universities also may need to protect patient data housed in teaching hospitals, confidential research findings and other sensitive material. Tests and quizzes must be safeguarded at all levels, of course. And like any large employer, educational institutions must protect the personal and financial data of workers.

All of this becomes more difficult as formerly closed educational networks are opened to a growing number of users. It's an environment where teachers and school staff must be much more vigilant about where and how they store information. Without proper policies and training, it's all too easy for inappropriately stored information to be discovered by unauthorized users. Training and awareness efforts should extend to students, as well. For instance, students need to be aware that information posted on social networks can be viewed by almost anyone and potentially used against them.

Automation can be a big help in understanding where sensitive data is stored, and what to do with information that's found in the wrong place. An effective data loss prevention solution should perform these functions:

- ***Discover —*** Find confidential data wherever it is stored, create an inventory of sensitive data and automatically manage data cleanup.

- ***Monitor —*** Understand how confidential data is being used, regardless of whether users are on or off the school network.

- ***Protect —*** Automatically enforce security policies to proactively secure data and prevent confidential data from leaving an organization. This can include blocking the ability to copy or transfer private or proprietary material, and warning users who attempt to perform forbidden activities.

- ***Manage —*** Define universal policies across the enterprise, remediate and report on incidents and detect content accurately within one unified platform.

Who's Accessing Your Network?

K-12 schools interact with a growing number of stakeholders electronically.

87% offer parental access to student grades online

32% maintain a presence on one or more social networks

86% offer online access to student attendance records

79% give students and staff members access to a 24/7 online school portal

82% provide online access to student homework

53% solicit public input via their website

SOURCE: 2010 DIGITAL SCHOOL DISTRICTS SURVEY

ENDPOINT SECURITY

A primary way for attackers to break into your network is by exploiting endpoint vulnerabilities. And with more students, parents and others gaining network access, the threat is continually growing for educational institutions. As they move toward an online and digital learning environment, schools need sophisticated endpoint protection that's simple to manage and cost-effective to deploy. Here are some best practices to keep in mind:

Find a comprehensive solution — Instead of deploying different solutions for different types of endpoints, look for one solution that protects all of the devices accessing your network. The solution also should combine core security technologies — anti-virus, anti-spyware, firewall, intrusion detection and prevention, and device and application control — into one integrated package.

Use behavior-based methods — These techniques study and react to the behavior of potential threats to deal with attackers proactively. These capabilities help safeguard network assets from ever evolving cyber-attack methods.

Look for advanced protection — It's important to deploy the most advanced security measures you can find, given the continual escalation in severity and sophistication of cyber-crime. Outdated security tools won't stop cutting-edge threats like rootkits, zero-day attacks and mutating spyware.

Use reputation-based security — Over the past decade, attackers have shifted toward more targeted threats. Instead of distributing a small number of common viruses across millions of users, today's attacks often use mutating threats that infect each user with a distinct variant. Traditional anti-virus tools that look for signatures of known threats struggle against this new type of attack. Reputation-based security uses global intelligence and sophisticated algorithms to compute a reputational score for a given piece of software. This method spots everything from common malware to the most arcane threat.

Demand simple management — Choose a solution that integrates a full range of security functions into a single software agent and offers a centralized management console. It should also offer an intuitive user interface and Web-based graphical reporting capabilities. Furthermore, these tools should give IT administrators the ability to set and enforce security policies across an entire campus or educational facility.

Case Study: Mobile County Public Schools

Keeping the network safe — no matter what kids download.

With its former security solution, Mobile County Public Schools coped with six or seven malware disruptions per year, requiring IT staff to spend as much as 300 hours annually on remediation. After a particularly bad experience with the Sasser virus, the school system switched to Symantec Multi-tier Protection. In the four years since, there have been no malware-related disruptions.

With 64,000 students in 94 schools, Mobile County Public Schools is the largest school system in Alabama. It's also one of the most technologically advanced school systems in the state and perhaps the entire southeast.

This stems from the school board's commitment to new technology — and also to a lucky real estate deal. A decade ago, the district acquired a state-of-the art facility in Mobile that was vacated by a local color printer manufacturer. "We were able to inherit their data center. And now we have a lot of the infrastructure that you would normally find at a Silicon Valley company," said George Mitchell, supervisor of IT for the district.

The result is that Mobile County Public Schools uses technology for just about everything. "We just installed NovaNET software for our Credit Recovery Program, which helps kids avoid summer school. We're installing 300 SMART boards in our classrooms. We maintain employees' time clocks; we have biometric fingerprint readers," Mitchell said. "Teachers can log in from home and see class demographics; students can log in and see their assignments."

One of the biggest challenges for Mitchell's 28-person IT department is administering and supporting 15,000 desktops and laptops used by the school system. "There are only 12 or 13 of us handling day-to-day operations and keeping the endpoints running," he said. "That's why we have to work extremely smart."

The district uses Symantec Multi-tier Protection, including Symantec Endpoint Protection and Symantec Mail Security for Microsoft Exchange. "A couple of years ago, I realized we had emerging threats: spyware, malware, different types of Trojans," Mitchell explained. "I didn't want to manage one product doing spyware, another doing viruses, and another doing a firewall."

The multi-tier solution is managed from a single console. Mitchell has an LCD monitor on his desk set to the console at all times, which lets him keep tabs on all security threats and responses.

"Today, it shows the solution blocked 45 viruses, cleaned seven and deleted 12. That's a fairly typical day," he said. "Because I can watch everything that's happening on the Symantec console, we can get more done with our small team."

The system also uses behavior-based analysis to stop zero-day viruses even before they've been identified and added to traditional anti-virus definition lists. "We have it set to quarantine any software that exhibits unusual behavior," Mitchell said.

Case Study: University of North Florida

Desktop management and endpoint protection solutions support a complex environment.

The University of North Florida (UNF) maintains some 3,700 desktop and laptop computers in an IT environment that poses both political and technical challenges. The university as a whole has an IT department, but the various colleges within UNF also employ their own technical staffs, and lines of responsibility and authority vary widely. More than 95 percent of the desktop and laptop hardware on campus comes from Dell. But the applications, configurations and security software on that hardware varies greatly.

Not long ago, the university used a variety of tools to manage its desktop clients and the software on them. "Being an educational institution, there's a lot of freedom here to do things you want to do, and to implement the products you want to implement," said Troy Whittaker, UNF's desktop systems specialist. "We really had a very fragmented systems management ecosystem."

Whittaker was assigned the task of determining the best way to manage the university's desktop environment in 2007. "I proposed the Altiris Client Management Suite, and we created a desktop systems team — that is, me — to run it," Whittaker said. "I'm a team of one."

UNF began deploying Symantec's Altiris notification server and deployment server, and migrating client images from other platforms into the Altiris database. The first pilot client deployment happened in summer 2008. "Then, throughout the fall and into January 2009, we did our Altiris agent rollout campuswide," Whittaker said. "Within three weeks, we had 95 percent coverage in our environment."

The success of the rollout enticed desktop managers in the individual colleges to join the Altiris effort. "Some folks have to use what we have to offer, but some folks don't — but they choose to because we offer some advanced operations," he said.

Whittaker also realized that the new desktop management solution could help with a pending universitywide upgrade to Symantec Endpoint Protection version 11. "I had investigated the integration component and knew that it was going to be powerful, so I asked [the team responsible for the upgrade] to wait" until Altiris was fully deployed, he said.

The Endpoint Protection upgrade was particularly complicated because clients used a variety of versions of Symantec Antivirus. The Altiris notification server allowed UNF to segment the machines based on those versions. "We upgraded more than 1,500 clients in something like 20 days without a single problem — no blue screens, no phone calls," Whittaker said. He estimates that the Endpoint Protection upgrade without Altiris would have taken four to six months.

Endpoint Protection does a superior job of protecting UNF's systems. "I can't think of a single time that we've had an issue that hasn't been immediately quarantined and remediated by Symantec," Whittaker said.

Simplifying Complexity With Endpoint Virtualization

It's clear that educational institutions face a significant challenge: More users will be accessing more information and network resources through an expanding variety of devices. Rapid growth of online and blended classes — along with a shift toward digital learning material — demands that students and teachers at all grade levels have computing devices and access to school networks. Moreover, the proliferation of personally owned computing devices — from laptops and tablets to smartphones — means many users will want to access your network with devices that you no longer control or manage.

These trends magnify a long-standing challenge for IT staffs at educational institutions, particularly at colleges and universities. Each fall, a quarter of the student population turns over, and hundreds or even thousands of new user devices must be configured with the right applications and access controls. K-12 education is feeling more of this pressure, too, as use of online classes and digital content grows at elementary schools and high schools. It's a support nightmare that's poised to worsen without a fundamental change in the management of client computer systems.

"Schools must adopt strategies that help them simplify the task of managing student computers and delivering digital content," says the CDE's Jackson. "This is an important requirement for increasing the use of online learning."

ENDPOINT VIRTUALIZATION: WHAT IS IT?

Endpoint virtualization is a strategy for reducing the complexity and cost of supporting end-user computing devices — and it's being adopted by a growing number of schools and universities. In a broad sense, endpoint virtualization separates the various functions involved in client computing into discrete pieces. So a user's data, configuration settings, software applications and operating system all become individual units that can be managed centrally and delivered to end-user devices on demand. Let's take a closer look at how endpoint virtualization fits into the evolving educational environment.

REDUCING MANAGEMENT OF END-USER DEVICES

Schools and universities need to spend less time managing pieces of end-user hardware. Traditional practices demand that only school-owned and managed computers gain access to network resources. Each of these machines must be maintained and supported by school IT staff. So IT personnel devote untold hours to loading applications on individual machines, updating those applications, resolving conflicts between them and maintaining operating systems. Sometimes IT departments spend days loading software onto school-provided computers before the start of a new semester. And given the number of machines being configured, it's inevitable that some will develop glitches that need further attention before they're ready for use.

Endpoint virtualization eliminates most of these chores by making the end-user hardware largely irrelevant. Applications are controlled centrally in an institution's data center. Individual applications or an entire student desktop can be delivered remotely and securely to any end-user device in any location. Support costs drop because school and university IT staffs spend less time trouble-shooting and updating software on laptops and desktops.

VIRTUALIZING AND STREAMING APPLICATIONS

Endpoint virtualization offers several options for giving users the software resources they need. For instance, it can support a thin-client model where end-user devices act as a terminal for applications that are housed and run in an organization's data center. With this approach, no applications actually exist on a user's desktop. Keystrokes and images are transmitted via the school's network between the back-end application and the end-user's device.

Another option uses technology known as application streaming to deliver applications to an end-user's device. Applications are delivered via wired or wireless networks, and they open and run on the user's desktop. This approach lets schools distribute applications to students for specific classes or projects and then retrieve those applications when students no longer need them. Distribution, support and management of the applications are controlled centrally.

Both endpoint virtualization strategies help schools simplify and strengthen management of end-user devices and software. Working in concert with network access controls, endpoint virtualization lets students, teachers and others log in to the network and receive a suite of individually tailored applications and information. These resources are linked to the user's identity instead of a specific device, so they can be safely delivered to any device with network access. The result is a richer, more convenient experience for users.

Just as important, applications and operating systems are managed and updated centrally. Complex programs — especially those used in research labs and other sophisticated environments — can take hours to install and configure on individual machines. And they demand even more attention when professors make changes. Endpoint virtualization allows these changes to be made centrally to a single virtual application, which is then delivered to end-user devices.

In addition, endpoint virtualization cuts the cost and hassle of managing software licenses through techniques like dynamic licensing. Instead of purchasing licenses to cover every potential user, institutions use dynamic licensing to assign software licenses only to students actually using the particular application. Students gain access to software resources they

Tech Support in Community Colleges

92% provide personal computing devices to full-time faculty

28% provide personal mobile devices to full-time faculty

74% provide tech support during business hours for full-time faculty

51% provide tech support for student laptops

SOURCE: 2010 DIGITAL COMMUNITY COLLEGES SURVEY

need for specific courses or projects, and access is revoked once the project ends and licenses are reassigned to the next group of users.

Getting Started

Endpoint virtualization offers a new strategy for delivering digital resources to end-users. Here are a few things to consider:

- Look for opportunities to separate software functions from hardware. Examine applications and data for potential virtualization.
- Evaluate your infrastructure. Streaming applications and rich media will put a premium on network bandwidth, reliability and availability.
- Evaluate your end-user device strategy and virtualize accordingly. Schools committed to providing full-function desktops and laptops can virtualize selected applications based on their needs. Schools adopting netbooks and other thin clients or supporting student-owned devices will require a greater amount of virtualization since these devices have less built-in computing power and may be unmanaged.

PROTECTING COPYRIGHTED AND TEST MATERIAL

The proliferation of online learning and growing use of digital textbooks introduces new concerns about protecting copyrighted content and preventing plagiarism and cheating. How do you keep students from posting the latest exam to a social network site? How do you ensure that proprietary digital learning material isn't shared inappropriately?

Endpoint virtualization coupled with security tools helps schools avoid these problems. Data leak protection technology can be incorporated into students' virtual desktops, preventing them from copying and pasting material. These tools also can restrict printing and block material from being downloaded to local computers and storage devices. The same technology can prevent teachers and staff members from inappropriately sharing student identities, medical information and other sensitive data.

DELIVER A BETTER USER EXPERIENCE

As technology becomes fundamental to the delivery of classes and learning material, users throughout the educational community will demand excellent performance and reliability from learning systems and devices. Without changing the paradigm for delivering IT-based learning resources, educators will be squeezed between user expectations and fiscal reality.

"Textbooks are going away; within five years, they'll be the exception, not the rule in many schools," says Halpin. "And low-cost tablet computers will revolutionize the learning environment. For the price of a couple of textbooks, you'll be able to buy a mobile tablet."

Approaches like endpoint virtualization position schools to take advantage of new digital learning strategies, enabling them to deliver a better user experience at a lower cost and with less complexity. Students, teachers and other users can log in to rich and sophisticated applications that include the latest updates and additions. Schools can stream Web design programs to support online website development courses. College students can access university-provided mathematical modeling applications while listening to a professor in a lecture hall or sitting in a coffee shop working on a research paper. And because they're much easier to support, these centrally managed applications will be more reliable and stable than software stored locally on end-user devices.

Just as important, streaming applications let schools support nearly any computing device. The technique relieves concerns about end-user operating systems, hard drive capacity, memory and other technical details. Students and teachers can use laptops, netbooks, smartphones or tablets to reach the resources they need.

Schools Depend on Technology

Common technology uses in K-12 school districts.

37% of students have district-allocated devices

87% of teachers take attendance electronically over a network

60% of classroom instruction is supported by presentation devices

52% of students use computers for presentations

SOURCE: 2010 DIGITAL SCHOOL DISTRICTS SURVEY

EMERGENCY PREPAREDNESS

The qualities that make endpoint virtualization an important strategy for online learning also prepare schools and universities to continue functioning during emergency situations. For instance, a flu pandemic could prompt closure of classrooms and administrative offices. Yet endpoint virtualization would give administrators, school board members and school employees access to all of their normal network resources from remote locations. Classroom learning activities also could be temporarily moved online.

Case Study: Rice University

Endpoint virtualization simplifies desktop support and enables software deployment on the fly.

Endpoint virtualization is generating quite a buzz among educational institutions, and for good reason: The ability to roll back applications to a standard image, avoid application conflicts and optimize license management can save thousands of hours per year in IT staff time.

"Educational institutions have been early adopters of endpoint virtualization because it addresses their major pain points," said Mark Bowker, senior analyst at Enterprise Strategy Group. "Traditionally a good portion of their IT staff time is spent on deployment — just rolling out new images. Endpoint management tools can lighten that load considerably, but there's a huge opportunity to reclaim staff time and improve service by virtualizing applications or workspaces."

Barry R. Ribbeck, director of systems architecture and infrastructure at Rice University in Houston, can relate.

"It's always a very challenging process for us to get images on the lab machines in a specific time frame," he explained. "There are so many different groups and people involved that the task is difficult at best, and deployment always comes down to the wire. And then once we have gone through all the effort to test and validate the image, there are inevitably last-minute requests or software versions that come out mid-semester that we're under pressure to accommodate. That's a tough position to be in, because we want to be responsive, but we can't risk application conflicts that might cause downtime for other users."

Ribbeck hopes that using Symantec Endpoint Virtualization Suite to stream applications to 500 desktop PCs in student labs will help solve these problems. Deployment of the solution is currently under way.

"Application virtualization will give us the ability to change horses in midstream and perform upgrades without impacting our base image," he said. "If an instructor wants to add software that's not in the default build, we'll be able to do that on the fly, without impacting every other course that's taught on those machines. We'll be able to provide instant gratification."

Case Study: St. Agnes Academy

Application streaming ensures that student computers are ready for class.

On the first day of school at St. Agnes Academy — a private all-girls school in Houston — more than 800 students have computing devices that needed provisioning. It's a task that used to overwhelm the academy's small IT team, reducing instructional time and creating challenges in license management. The school turned to Symantec for a solution that streams applications on demand and manages licenses centrally. Results include a 40 percent reduction in help-desk tickets, two to five days reclaimed in instructional time per class, and 100 percent payback in four months.

PHOTO COURTESY OF ST. AGNES

All St. Agnes Academy students carry and use portable computers, wirelessly connected with school servers. It's been a tradition since 2001, when the school became one of the first in the Houston area to adopt a one-to-one computing program. Here's how it works: Every incoming freshman buys her own device — in 2008, the approved model was a Fujitsu tablet PC — and uses it throughout her school years both on campus and at home to enhance instruction.

The school maintains the students' computers and supplies them with needed applications. Learning can't start until student devices are loaded with the right applications and e-books. Solving this challenge falls to Director of Technology Jason Hyams and his team of three IT technicians. They're assisted by a technology coordinator who also trains and teaches.

Hyams came to St. Agnes from the corporate IT world with a personal mission: Take a technology-aware school and make its infrastructure even more useful, increasing educational value. He and his team have made progress. The wireless network used to support only 300 concurrent users; now it can support more than 750 concurrent users. It once was a challenge to sign on to the network, and there was no easy way to share documents. The IT team received frequent calls for password reset help. Now there's a self-service portal accessible from any Web browser, it's easy to share and store documents centrally, and users perform self-service password resets.

"It's really about simplification," Hyams said.

Online Learning Infrastructure

Greater use of digital content and the implementation of endpoint virtualization put growing importance on campus computing infrastructure. Web conferencing and streaming video are crucial to blended and online courses, but these applications place greater demands on network bandwidth and storage capacity. The virtualization of end-user applications enables schools to simplify support and offer rich services to in-class and remote users. But similarly, streaming applications and other resources across your network requires ample and reliable bandwidth. And these centralized applications need to live in efficient, highly available data centers.

Indeed, as schools and universities move toward online and blended course models, they'll be under mounting pressure to make sure learning resources and student services are available every day, around the clock. This section highlights some infrastructure best practices.

NETWORKING SYSTEMS

Converged networks are now the standard for campus communications. These networks use the Internet protocol (IP) method for delivering voice, data and video applications across a single, unified communications infrastructure. This approach should cover both wired and wireless communications. Using a converged network architecture makes network implementation cheaper and more flexible. At the same time, it allows for better network management and stronger security. If they haven't already, schools should consider moving toward converged networks to control costs and accommodate new services and applications.

Wired networks remain the backbone for campus communications. These systems generally operate at speeds ranging from 10 Gbps in the data center to 100 Mbps for end-users. Campus wired networks also can incorporate sophisticated switches with access controls and user authentication features that protect school information systems from inappropriate use. Although wireless services are common on school campuses, they usually are connected to and rely upon the wired network. Here are a few other features to consider:

Quality of Service — As the use of voice and video content grows, school networks need the ability to prioritize communications traffic to provide the best service for all users. This capability is known as Quality of Service (QoS). For example, QoS allows networks to understand that video content is more sensitive to time lags than pure data traffic and adjust transmission speeds accordingly. QoS also can prioritize network traffic based on user types, time of day and other factors.

Power over Ethernet — This technology allows the network to power devices such as wireless access points and telephone handsets. In other words, power is provided through the same wiring that connects the access point to the network, eliminating a separate electrical connection. This can help schools cut electrical installation costs and operating expenses.

Video on Campus

Here's how community colleges say they are using campuswide video distribution:

Multidirectional video conferencing	**87%**
On-campus video editing capability for curriculum	**75%**
On-demand access to video assets	**74%**
Live campus-originated video feeds	**73%**
Live television from broadcast, cable, etc.	**58%**

SOURCE: 2010 DIGITAL COMMUNITY COLLEGES SURVEY

DATA CENTER

Data center consolidation is a key trend for schools and universities, both for containing costs and improving support for vital applications. Traditionally each software application had its own server, which forced organizations to operate large numbers of servers that all had be provisioned, managed and maintained separately. In addition, these servers often were located near users to reduce network demands and connection costs. Vast improvements in processor performance and network capacity are changing this model, allowing educational institutions to centralize computing resources in efficiently managed and well protected data centers.

In higher education, it's becoming more evident that integrated and strategic server consolidation is essential for effective IT management and cost reduction. Similarly, K-12 school districts are centralizing computing resources to maximize processing power and stretch limited human resources in IT departments.

Server virtualization often accompanies consolidation efforts. This technology uses software to create multiple virtual servers on a single piece of server hardware. As a result, one server can efficiently support multiple applications. Virtualization reduces the number of servers organizations need to operate their applications. This strategy helps educational institutions dramatically cut expenses for equipment, energy, facilities and management. It also improves the reliability and flexibility of key digital services.

STORAGE

By some accounts data storage on campuses is growing by more than 50 percent annually, driven largely by increasing digital content use in the classroom and online. Clearly this trend will continue as schools move toward blended courses and distance learning models. Schools also are retaining more student records, including projects and assessments, as well as storing data needed to comply with state and federal regulations.

A number of technologies aim to improve storage capacity and efficiency. For instance, storage area networks (SANs) allow storage capacity to be shared among several network-connected storage devices. And content addressable storage (CAS) systems retrieve data based on its content instead of storage location, providing more efficiency for storing information that doesn't change over time.

Schools also need to develop storage policies that limit access to sensitive data, while making allowable information easy for users to search and retrieve. Storage solutions must be available to students and staff via a wide range of devices. In addition, parents and administrators should have simple access to relevant data on student progress.

Regulatory Considerations

School and university information systems possess significant amounts of sensitive data. This information is protected by a growing number of federal and state regulations. Sophisticated access controls and security solutions are vital for complying with these mandates, especially as campus networks offer expanded access to growing numbers of users. In addition, educational institutions need to develop information policies and employee training programs that respond to these requirements. Here are some significant regulatory issues to keep in mind as you develop online learning strategies:

***Federal Educational Rights and Privacy Act (FERPA)* —** This federal law protects the privacy of student education records. It applies to schools that receive funds from programs administered by the U.S. Department of Education. Under FERPA, schools need a student's consent before releasing his or her educational records. Parents of students under the age of 18 receive certain access rights. There are other exceptions too. For instance, records can be released to school officials with legitimate educational interests,

for financial aid purposes, to schools where a student is transferring, and to health and safety officials. Educators must be familiar with FERPA requirements, especially as they make a growing amount of student data available through online portals.

Children's Internet Protection Act (CIPA) — This law is intended to block offensive Internet material from children using school and library computers. It applies to schools and libraries that receive funding from the federal E-Rate program. Schools and libraries must certify that they have deployed technology tools to block or filter offensive material from computers used by minors. Schools subject to CIPA also must adopt and enforce a policy to monitor online activities of minor children. In addition, schools and libraries must implement Internet safety policies. These policies need to address access by minors to inappropriate Internet content; safety and security while using e-mail, chat rooms and other electronic communications; hacking and other unauthorized or illegal online activities; and several other topics.

Health Information Portability and Accountability Act (HIPAA) — This federal law, enacted in 1996, sets national standards and requirements for electronic health-care transactions. It includes provisions designed to protect individuals' health records and other identifiable health information by requiring appropriate privacy protections. Schools can be subject to HIPAA requirements if they operate student health clinics, conduct certain types of Medicaid transactions or in other situations. But the interplay between HIPAA and FERPA can be complex. Administrators need to understand these laws and their implications — and then design access and security policies accordingly. In addition, university hospitals clearly must deal with HIPAA requirements.

State Cyber-Bullying Legislation — A growing number of states are considering laws to prevent school-age children from being attacked electronically by classmates and acquaintances. The issue drew national attention last year when a 13-year-old Missouri girl committed suicide following an Internet hoax. Use of popular social networks to spread rumors and other negative information has generated a flood of complaints from students, parents and educators. That's prompting lawmakers nationwide to draft legislation giving schools more power to stop electronic bullying. Most of these laws target the use of school computers and networks, according to recent coverage in *USA Today*. But others call for education officials to take action against off-campus incidents that disrupt school activities. It's unclear how these initiatives will evolve, and some proposals are drawing opposition from free-speech advocates. Educators will need to monitor these activities and be prepared to respond to new requirements as they emerge.

For additional copies or to download
this document, please visit:
www.convergemag.com/e-learning