

SonicWALL K-12 Education Solution Brief

EDUCATION

Protecting K-12 Students and Schools from the Risks of Web 2.0

Technology can drive K-12 educators and staffers to distraction, especially when it diverts attention and resources from the core mission of teaching. The so-called “Web 2.0” phenomenon is a prime example of technology as a two-edged sword. Its new, innovative ways to collaborate between teachers, students and parents have also exposed dangers that can harm students and schools alike. This article shares ideas on how K-12 districts can safeguard Web 2.0 activity.

Promise of Web 2.0

Loosely speaking, Web 2.0 is the family of Hypertext Transfer Protocol (HTTP)-based applications such as social networks, blogs, wikis, instant messaging, streaming video and audio, peer-to-peer sharing, and RSS feeds. It’s a huge phenomenon because after years of gradual enhancements to Web standards and applications, suddenly—everything is finally working together in a global, uber collaboration. Web 2.0 applications allow educators and students to leap beyond old walls and ways of learning. Decades from now, historians may well look back to this era as the dawn of a new age in education.

Practical Applications

The convergence of Web 2.0 technologies enables convenience and collaboration. Educators can leverage the power of Web 2.0 by instantly tapping lesson resources that used to take weeks, months or years to synthesize into a useful format. Peer collaboration is now effortless, whether an associate is across the hall, or across the continent or globe. Outside experts can easily participate as guest lecturers with the click of a mouse.

Students now enjoy similar versatility in finding resources for research, learning, and writing. Students used to have few chances for broad exposure and sharing of their ideas. Now, they can instantly self-publish results in multimedia formats available to anyone with a browser. Web 2.0 does not replace classroom instructors, but it sure has made dusty lecture notes and outdated textbooks looking passé. Parents too can use Web 2.0 for scholastic collaboration. Forget the one-chance-per semester limitations of Parent Night. If they so desire, parents can participate in their children’s’ learning every day in real time—thanks to Web 2.0.

“SonicWALL gave us comparable high-performance security features for everything we needed, and was still much less expensive than all the other products we looked at.”

Darin Hostetter
Technology Coordinator
Marshall, Illinois School District

Understanding the Nature of Web 2.0 Risks

With these positive benefits come several risks that can bring harm to students, to their confidential personal data stored in school district administrative databases, and possibly to the health of a district’s network and IT assets.

The risks of Web 2.0 differ from traditional breach vectors such as viruses or worms entering the district network via email or an infected file, or hackers leveraging software vulnerabilities in operating systems, commercial applications, open-source code libraries, and Internet protocols. For these risks, your district can deploy security controls such as firewalls, intrusion prevention, virtual private networks for remote access, anti-virus, and anti-spyware.

Web 2.0 risks raise the ante because they can bypass traditional controls and strike your students, faculty, administrators, and indirectly the parents and others connected to your district network via any HTTP application.

Blocking Web 2.0 Proxies

A proxy is a Web site acting as a relay. An individual logs onto a proxy, which in turn establishes an encrypted SSL connection to a different Web site. Proxies are a big problem. Students use them to mask their identities and sidestep a district’s controls for preventing use of forbidden Web sites or Web 2.0 services. These include video streaming services, gaming, pornography, or social media. The latter is especially risky as it exposes students to potential predators. Like other Web sites, access to proxies can be banned by adding their URL address to a district’s blacklist. The challenge is that proxies often change addresses, sometimes on a daily basis. As a result, network administrators are forced to play a constant game of catch-up.

“SonicWALL enables us to keep up with the many new Web sites appearing daily that may need to be filtered. Plus, by eliminating traffic to undesirable sites, we can free-up bandwidth for legitimate school activities.”

Dennis Peterson
Technical Services Manager
Kansas City, Mo. School District



To effectively block proxies, district network managers should consider automating as many relevant security controls as possible. Your network and Application Firewalls should build in detection of proxy servers. Ideally, the solution should be capable of reading SSL packets for automatic detection of flows going to forbidden sites. It is also important to automate updates to firewall configurations and blacklists for remote sites. Otherwise, you will be sending a team of administrators every day to update configurations at each school and administrative building in your district.

Strategies for Minimizing Other Web 2.0 Risks

Minimizing risks from Web 2.0 requires controls for managing the use of Web applications, data, and networks. The term “use” should extend beyond students to include faculty and staff because all Web 2.0 users can bring in harm, even if their activity is not intentionally malicious.

Applications and Data. Use network bandwidth management to identify and control different kinds of network traffic—malware or good, application or data, wasteful or productive. Content filtering can help you accept or reject different file types and Internet content, such as music files or video downloads. These controls can also prevent inappropriate content in schools, such as pornography, games, gambling or online shopping.

Streaming Video. Sites such as youtube.com can be banned, but many also feature content that can be useful in an educational context. Consider controlling use of streaming video by limiting bandwidth. A deep packet inspection engine can examine HTTP headers to spot and control the flow of streaming video. Permissions can be granted on demand to prioritize these flows in case they are required in a particular classroom context.

Keep P2P Apps Under Control. Peer-to-Peer application such as BitTorrent can steal bandwidth and allow inflow of mischievous files. Deep packet inspection tools can also control use of Peer-to-Peer (P2P) applications just like streaming video.

Block Forbidden Files and Notify. Your district must have a firewall that can block passage of files with potential for causing damage, including EXE, PIF, SRC or VBS. Create a “forbidden file extensions” list and implement a blocking policy that is enforced with deep packet inspection.

Easing Deployment and Management of Web 2.0 Security

Security is not a “core competency” for school districts, yet expectations for protecting students, their data, and district IT assets are constantly rising. With these new operational burdens, cost containment through lower capital expenditures and better operational efficiency is essential. For this reason, solutions for Web 2.0 security should be simple to deploy and manage.

Many districts have chosen the “security gateway” approach, which entails deployment of appliances with Unified Threat Management (UTM). SonicWALL® is a leading Unified Threat management firewall provider. Its UTM solutions provide a centralized model that entails a single box integrating all necessary security applications—including protections for Web 2.0. SonicWALL’s UTM replaces the old inefficient, expensive model of deploying and managing multiple servers and security applications, and manually integrating operational data for compliance reporting.

SonicWALL UTM’s are deployed at the network edge for comprehensive coverage of threats inside and outside the district. They are centrally managed with one simple interface. A huge operational benefit to UTM’s stems from built-in integration—it automates the synthesis and rollup of enterprise security data, which makes fulfillment of reports for security compliance a simple, fast procedure.

With Web 2.0, schools are on the cusp of a major innovation in teaching and learning. By leveraging security controls such as the SonicWALL UTM firewall appliance, districts can ensure the safety of students, their personal data, and valuable IT assets—and establish a technological foundation for a new era of learning.

“SonicWALL enables me to manage with a small staff. I don’t need to send people to every school to implement firewall and filtering updates.”

Dennis Peterson
Technical Services Manager
Kansas City, Mo. School District

SonicWALL for Strong Web 2.0 Security

SonicWALL provides leading appliance-based security solutions for Web 2.0. Solutions scale from small and mid-sized school districts to the largest educational institutions. SonicWALL includes a full range of security controls to ensure safety and protection for Web 2.0.

SonicWALL’s line-up of comprehensive protection



NETWORK
SECURITY



SECURE
REMOTE ACCESS



WEB AND E-MAIL
SECURITY



BACKUP
AND RECOVERY



POLICY AND
MANAGEMENT

SonicWALL, Inc.

2001 Logic Drive, San Jose, CA 95124
T +1 408.745.9600 F +1 408.745.9300
www.sonicwall.com