# VULNERABLE NO MORE: HOW TO SOLVE COMMON K-12 SECURITY CHALLENGES

## K-12 At a Security Crossroads

It's no secret that school districts are a gold mine of confidential student, parent and employee data that cybercriminals can exploit for financial gain or personal grudge. These hackers can be single individuals, organized criminal gangs, nation-state actors or even students themselves. For example, the personal information of about 15,000 students was posted to an online forum after a breach at Long Island's Sachem Central School District. The suspected culprit? A local high school student. And at Prince George's County Public Schools in Maryland, an intrusion by an unknown cybercriminal compromised the personal data of 10,000 employees. A private sector report says educational institutions experienced 165 data breaches in 2014, and that 65 resulted in confirmed data loss.[1]

K-12 networks and network endpoints can be particularly vulnerable to attacks. The increasing use of student computing devices and online learning and testing platforms has created an evolving, complex and costly security burden. It's difficult to manage and protect interconnected, multi-campus networks. Districts must also comply with the Children's Internet Protection Act (CIPA) to be eligible for federal E-rate funding for Internet access technologies.

Although the stakes are high, sadly, budgets are not. According to a Consortium for School Networking (CoSN) survey, 70 percent of K-12 technology administrators say their budgets have either plateaued or decreased.

## Common Security Concerns and Challenges

K-12 districts struggle with a number of vexing security challenges, including:

**Internal and external breaches.** External cybercriminals seek Social Security numbers and financial information, while student hackers commit inside jobs with the hope of changing grades, shutting down systems or posting personal information.

These threats constantly evolve. For example, a new type of breach, called "ransomware," expands beyond data theft into extortion. Hackers encrypt network and server data; for a large sum of money, they will provide the decryption keys. If the ransom is not paid, they permanently destroy the data.

## SNAPSHOT OF SCHOOL CYBERCRIME

- At Long Island's Sachem Central School District, it is suspected a high school student hacked into the personal information of about 15,000 students and posted it to an online forum.
- At Prince George's County Public Schools in Maryland, an intrusion by an unknown cybercriminal compromised the personal data of 10,000 employees.

**Technology advancements.** Digital learning tools and apps, online testing and 1:1 computing initiatives are immensely valuable, but consume bandwidth and add layers of complexity to network administration.

Students want to use their network-connected devices for non-education websites, which can include inappropriate and harmful content and bandwidth-draining applications such as streaming music and video. What's more, tech-savvy students can override device and application security features that prevent them from using blacklisted websites, content and applications.

**Multi-campus networks.** A typical school district has multiple school campuses that are interconnected through the Internet. Managing complex school district networks is time consuming and expensive, because each site must be equally protected by multiple layers of security technology.

**Outdated wireless networks.** Many schools haven't upgraded their wireless access points (APs) to the new 802.11ac standard, which provides better reliability and higher throughput. Outdated networks have spotty coverage, lack the bandwidth and performance needed to handle today's devices and multimedia content, and are frequently plagued by confusing security and access procedures.

Today's tech-savvy students will often find ways to override security features so they can use their network-connected devices for non-education websites. However, these websites can sometimes include inappropriate and harmful content.

When faced with a slow browsing experience and a complicated interface, students (and even teachers) may take matters into their own hands. When users disable security features, bypass important security steps or connect their own APs to the school network, they compromise network security.

**Since 2008, local school districts have reduced the number of public K-12 teachers and other school workers by 297,000 while the number of students has increased by about 804,000.**

**CIPA compliance.** Compliance with federal and state mandates and security standards is another strain on school districts. In particular, CIPA requires them to filter harmful online content as a condition for receiving federal E-rate funding, which provides much-needed discounts on telecommunications and Internet access services.

**Scarce resources and expertise.** Schools and districts face an ongoing scarcity of funding, and rarely have enough budget dollars to support all critical technology initiatives.

The K-12 budget gap extends to the personnel office. Since 2008, local school districts have reduced the number of public K-12 teachers and other school workers by 297,000 while the number of students has increased by about 804,000.[2] This means fewer qualified IT staff, especially those with cybersecurity experience.

## Shift the Security Burden with an Integrated Solution

In spite of these challenges, managing and maintaining a secure learning network doesn't have to be difficult. The SonicWall platform provides a secure remote and on-campus network access and integrates the critical functionality school districts need, including:

- ✓ Firewall
- ✓ Security services (e.g., anti-virus, intrusion prevention, application control, content filtering)
- ✓ High-speed wireless access points
- ✓ Caching of frequently visited websites
- ✓ Central management of all network devices

**The SuperMassive and NSA Series** are next-generation firewalls (NGFWs) that control internal network traffic like a traditional firewall, while providing additional layers of security, including intrusion prevention, anti-virus protection, malware and spyware blockers, and application intelligence and control.

Leveraging deep packet inspection (DPI), SonicWall NGFWs automatically examine every data packet passing through the network at a deeper level than traditional firewalls.

DPI also inspects encrypted Secure Sockets Layer (SSL) traffic to block malware hidden in the encrypted traffic, a process known as DPI-SSL.

DPI technology detects hidden application vulnerabilities that may let in attackers. It also allows IT administrators to prioritize critical learning applications and throttle or completely block social media, gaming, streaming video and other applications that hog the network or contain potentially harmful content.

Finally, DPI provides intrusion prevention that prevents hackers from finding network backdoors, as well as real-time gateway anti-virus scanning and dynamic spyware, spam and phishing protection.

The NSA Series is designed for small- and medium-sized multi-campus districts, while the SuperMassive Series meets the security and performance needs of larger branch campuses, including those with centralized data centers. Because all SonicWall firewalls use the same DPI technology and provide the same security services, districts are protected equally, regardless of their size.

For CIPA compliance, the **Content Filtering Service (CFS)** is integrated into all SonicWall NGFWs. CFS allows school districts to control websites visited by school-issued and personal devices connected to the Internet through the school network's firewall.

SonicWall CFS compares requested websites against a cloud database containing millions of rated URLs, IP addresses and websites. Via CFS, IT staff can create policies that allow or deny access to sites based on individual or group identity or time of day.

For laptops used outside the firewall perimeter, the SonicWall Content Filtering Client addresses safety, security and productivity concerns by extending the controls to block harmful and unproductive Web content. The client is automatically deployed and provisioned through a SonicWall firewall. This means schools can ensure they are still complying with CIPA regardless of whether students use school-issued devices at school, at home or somewhere else.

To protect wireless networks, SonicWall provides a wireless network security solution that combines next-generation firewalls with high-speed 802.11ac **SonicPoint Wireless Access Points.** This combination forces wireless traffic through the firewall where it is scanned for threats, ensuring wireless and wired networks are equally protected.

Seamless integration with the next-generation firewalls simplifies network setup and management — the APs are automatically detected and provisioned by the firewall. The wireless LANs in each school are now protected by DPI, DPI-SSL, intrusion prevention, content filtering, and other comprehensive features and services.

## SONICWALL SECURITY SOLUTION

Firewall

### SUPERMASSIVE AND NSA SERIES

**Next-generation firewall technology**

Web Filtering

### CONTENT FILTERING SERVICE (CFS)

**Block access to harmful Web content**

Wireless

### SONICPOINT WIRELESS ACCESS POINTS

**High-speed wireless network integrated with firewall that automatically scans traffic**

WAN Acceleration

### WAN ACCELERATION (WXA) SERIES

**Web caching increases browser response times and improves application performance between sites**

Management

### GLOBAL MANAGEMENT SYSTEM (GMS)

**Monitor and manage SonicWALL devices and services from a single dashboard**

A key performance-related component of the SonicWall solution is the **WAN Acceleration Appliance (WXA) Series**, which leverages Web caching to provide fast access to frequently visited websites. Frequently visited website pages are cached on the WXA and served locally, which saves bandwidth and loads websites faster. In addition, the WXA series accelerates application performance between multiple campus sites across a district's WAN.

Finally, the **Global Management System (GMS)** is a centralized management tool for multi-campus network security and wireless LANs. It enables IT staff to deploy and manage all SonicWall security devices and services across multiple sites from a single dashboard, and provides real-time and historical reports on network activity to deliver greater network insight. These reports can help IT staff identify abnormalities, suspicious behavior and other potential threats.

## Integrated Security Solution Maximizes IT Investment

**The SonicWall security solution** provides K-12 school districts with a number of improvements to network security and performance:

- ✓ **Complete, integrated portfolio.** Because its components are seamlessly integrated, SonicWall is cost effective and easy to deploy and manage, without sacrificing network protection for high performance.
- ✓ **Improved security against advanced threats.** SonicWall's DPI technology creates a firewall perimeter that blocks cyber attacks, and provides integrated anti-virus, spyware and malware blockers and intrusion prevention.
- ✓ **Secured wired and wireless networks across multiple campuses.** Combining the wireless network and firewall provides equal protection for wireless and wired networks across multiple sites.
- ✓ **Higher performance.** Websites load faster with local caching, which also preserves network bandwidth for critical applications.
- ✓ **Content filtering and CIPA compliance.** IT staff can monitor and enforce internal Web use policies on school-issued devices inside or outside the district firewall, which helps schools achieve CIPA compliance and E-rate eligibility.
- ✓ **Centralized management.** The SonicWall solution helps stretch thin IT resources by simplifying deployment and administration.

A recent Walton County Public Schools security deployment showcases many of these benefits. To replace a slow, unreliable firewall that was impeding performance, the Georgia-based district turned to SonicWall to provide a more reliable solution for 14,800 network users across 15 different campuses. "The SonicWall SuperMassive will easily support our district's 5,000 devices connecting to it and surfing the Internet at the same time, which was important to us. It doesn't even break a sweat," says Jon Graves, the district's technology services coordinator.

With a SuperMassive firewall in place, the district has 10 times the performance with no downtime. It's also reaping the benefits of integrated anti-virus, spyware and malware blocker, intrusion detection and content filtering, which was even more apparent after using the firewall to roll out 4,000 tablets to high school students. Notes Graves, "Whenever students go home, we have the [tablets] set up to go through SonicWall in order to access the Internet, so they're still getting their content filtering and the assurance of reliable, fast Internet access."

## SONICWALL AND E-RATE ELIGIBILITY

The E-rate discount program for funding telecommunications, Internet services and internal connections is an indispensable source of funding for K-12 schools, especially those in higher-need or rural areas. E-rate has two funding categories:

- Category 1 includes technologies and solutions for telecommunications, Internet access, WANs and phone service
- Category 2 includes internal broadband connections, maintenance of internal broadband connections and managed internal broadband services

SonicWall solutions are eligible for Category 2 funding. An internal broadband connection as defined in E-rate documentation includes WLAN access points, caching, firewalls, and supporting software and maintenance.

Centralized management makes it easy to manage security functions and it takes less time to make changes to the firewall, allowing IT staff to be more efficient and proactive. "I frequently make a lot of firewall changes. It's not uncommon for me to make up to six changes a day, such as allowing user access to an application or unblocking a website," says Graves. "It used to take me 15 minutes and now it takes me 30 seconds from start to finish."[3]

## Conclusion: Realizing a Safe and Secure Digital Learning Environment

Increasingly sophisticated threats from inside and outside the network, combined with digital learning advancements, have created a watershed moment in school district cybersecurity. But as school and district IT staff work to deploy, manage and maintain technology-based learning initiatives, they're faced with mounting budget and staffing challenges that too frequently lead to an inadequate security effort.

One solution is the SonicWall E-rate-eligible security platform for K-12 school districts. School districts can rely on SonicWall education solutions to help them realize the promise of technology without sacrificing network security or performance.

### Endnotes

1. http://www.verizonenterprise.com/DBIR/2015/
2. http://www.cbpp.org/research/state-budget-and-tax/most-states-have-cut-school-funding-and-some-continue-cutting
3. http://www.sonicwall.com/documents/school-district-speeds-performance-tenfold-casestudy-25822.pdf

### About Us

Over a 25 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.

For more information about SonicWall solutions for education, visit **www.sonicwall.com/solutions/education**

Sponsored by: SONICWALL®