About

This white paper examines the key security requirements that are emerging for BYOD (Bring Your Own Device) implementations in schools. It reveals ContentKeeper's approach to these requirements and why this approach offers significant advantages over other offerings.

After reading this white paper, the reader should have a greater understanding of the implications of BYOD adoption for school networks—and the factors necessary for mobile web security.

White Paper

Enabling BYOD in Schools with Seamless Mobile Device Accountability & Control

How to support students' use of personal mobile devices while maintaining web security and policy compliance in schools

Introduction

The proliferation of smart phones, tablets, and other web-enabled mobile devices has dramatically altered the education landscape, transforming how students use online learning resources. Students are no longer physically tethered to workstations in classrooms or computer labs; instead, they can access the web and learn from wherever they are, at home or at school, using a wireless network environment.

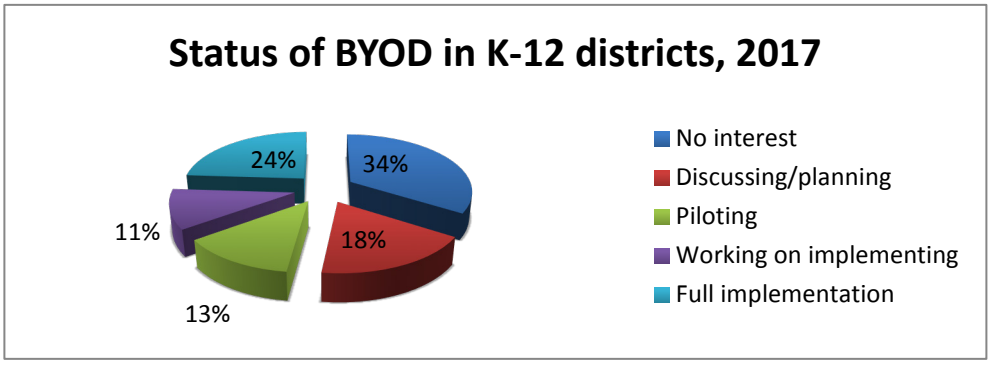
To save money and leverage the devices that students already own, many school systems have adopted a Bring Your Own Device (BYOD) policy, in which students can use their own personal smart phones, laptops, or tablets to connect to their school's network. However, BYOD policies also bring serious compliance and IT security risks.

School leaders must make sure their students aren't introducing malware or other threats to their network through an unsecured personal device. They also need a way to ensure compliance with the school's Acceptable Use Policy (AUP) and the Children's Internet Protection Act (CIPA) when students are using a personal device to get online.

What schools need is a simple solution for securing BYOD access in educational environments that is flexible, proven, reliable, and easy to implement and support.

BYOD and Security Risks

BYOD has grown rapidly in schools. According to a 2017 survey of K-12 chief technology officers by the Consortium for School Networking (CoSN), the percentage of districts with "fully implanted" BYOD programs is now 24 percent—up from 16 percent the previous year. Altogether, two-thirds of K-12 districts are at least discussing or planning BYOD policies, the survey indicates:



The same CoSN survey suggests that cyber security is a growing concern for K-12 leaders as well. Cyber security was the No. 3 concern for school IT leaders in 2017, ranking behind only mobile learning and broadband/network capacity. Sixty-one percent of respondents rated cyber security as more important than last year, and 30 percent said it was "much more important."

Fueling these concerns is the fact that schools have been victimized by several high-profile malware attacks in recent years. According to security analyst BitSight in its 2016 report "The Rising Face of Cybercrime: Ransomware," education is now the sector that is most often targeted by ransomware attacks, which hold networks hostage until a ransom is paid.

School leaders need a way to provide secure, filtered web access to students who are using their own devices at school, without compromising the school's network. A proper BYOD strategy enables school IT administrators to identify each network user, enforce the right policies for that student, report on the student's network activities, and keep malware from infecting either the student's device or the network—without requiring major network configuration changes or headaches.

How ContentKeeper Can Help

ContentKeeper has the solution to BYOD security in education. The company's Multi-layered Gateway Security Platform gives school leaders an easy way to centrally manage their students' web access and secure both devices and networks from the latest online threats—regardless of whether students are using personal or school-issued devices.

ContentKeeper provides advanced threat protection, malware defense, accurate device identification and reporting, and a versatile set of browsing and usage controls. It's an in-line solution that uses a Layer 2 Ethernet bridge design for deep packet inspection and filtering of all web traffic, which means it is device-agnostic. What's more, ContentKeeper integrates with the leading authentication and directory services used by school districts, so it can apply web policies to a device based on the user's system profile.

Because ContentKeeper can enforce policies and inspect web traffic sent to and from any device, at any location, school leaders can safely and confidently protect their networks from the security threats posed by BYOD—while also remaining CIPA compliant.

A Closer Look

ContentKeeper's flexible solution can be configured in different ways, based on a school system's needs. The process for authenticating a student connecting to the network from a personal device depends on the network administration tools used by the school or district, but in all cases the goal is a simple and streamlined experience for end users.

For schools using Remote Authentication Dial-In User Service (RADIUS) or Cisco Identity Services Engine (ISE) software, the authentication process is seamless and occurs in the background automatically. In other cases, when a student tries to access the network, an authentication page appears in the device's web browser. Students can enter their network username and password to receive their normal network privileges enforced on that device, or if they are a guest user they can ignore this request and be treated as an unauthenticated user. In that scenario, the default browsing restrictions can be set by the school or district.

Once a device is authenticated, ContentKeeper applies the appropriate web policies for that user—and it provides full reporting and accountability. System administrators receive web usage reports and real-time alerts that contain not only a device's MAC address, but also the username associated with that device.

Here are some of the system's powerful features:

- ***Advanced threat protection***. ContentKeeper scans web traffic for malicious content in real time. It includes predictive malware blocking capabilities powered by Cylance, and it can be set up to block users' access to known malware sites and websites with invalid SSL certificates.

- ***Threat isolation***. If ContentKeeper sees that a device is infected with malware, the system can isolate that device so it can't communicate on the network until the problem is resolved.

- ***Web policy enforcement***. ContentKeeper provides very granular web access controls. Administrators can set policies based on specific user groups, so students at different grade levels can be given access to different types of materials. And this granularity applies to Web 2.0 and social media tools as well, letting administrators block access to certain types of content while allowing others—even within the same website. That means students can be given access to educational videos on YouTube, while being restricted from non-educational content.

- ***Keyword monitoring and behavioral intent alerting***. Keeping students safe while they're accessing the Internet is important, but so is keeping them safe from physical harm. ContentKeeper scrutinizes students' Internet searches for indicators of potentially harmful behavior, such as threats, bullying, drug or alcohol use, sexual assault, and thoughts of suicide—and it delivers real-time alerts to designated administrators so they can follow up on these instances as appropriate.

For schools to take full advantage of these capabilities, students must install a trusted certificate for Secure Socket Layer (SSL) decryption on their personal devices. This certificate allows ContentKeeper to decrypt and inspect SSL web traffic, which includes nearly all social media interaction and queries to Internet search engines. Once students are authenticated, they will receive instructions for how to install the certificate, which is tamper-proof. School systems can require installation of the certificate before granting network access to a student-owned device.

System Administration

ContentKeeper can be managed easily from a central console. Authorized IT administrators can create any number of student groups and can define Web access policies for each of these groups.

Students typically are authenticated for as long as their Web browsing session remains open. Flexible options within ContentKeeper allow schools to set time-out periods, requiring reauthentication once a session is inactive for a certain period of time. Or, if preferred, ContentKeeper can be configured to "remember" student devices—and every time a device is seen on the network, it can be linked to the registered user account automatically.

ContentKeeper continually tracks web use for each device. Network administrators can see, at a glance, what devices are being used on the network, by whom, and for what purposes. Administrators can see:

- What type of device is being used and the manufacturer.
- What software version of the operating system is installed.
- Which user is browsing on the device and how he or she was authenticated.
- How long the user has been browsing the web in the current session.
- The device IP address and MAC address.

In Conclusion

ContentKeeper allows schools to seamlessly support BYOD environments with centralized device management, filtering, and security—without requiring special client software or costly disruption to their current IT infrastructure. ContentKeeper's in-line Layer 2 Ethernet Bridge design works with any existing network architecture and can be hosted in the cloud if desired.

ContentKeeper can enforce web filtering, security, and acceptable use restrictions on workstations, smart phones, laptops, Chromebooks, and tablets. No matter where students are located, or what devices they are connecting from, school leaders can confidently support BYOD and open their networks to students' personal devices.

To set up a free demonstration email:
k12@contentkeeper.com

ContentKeeper.com k12@ContentKeeper.com US: +1 888.808.6848 Intl: +61 2 6261 4950

ContentKeeper