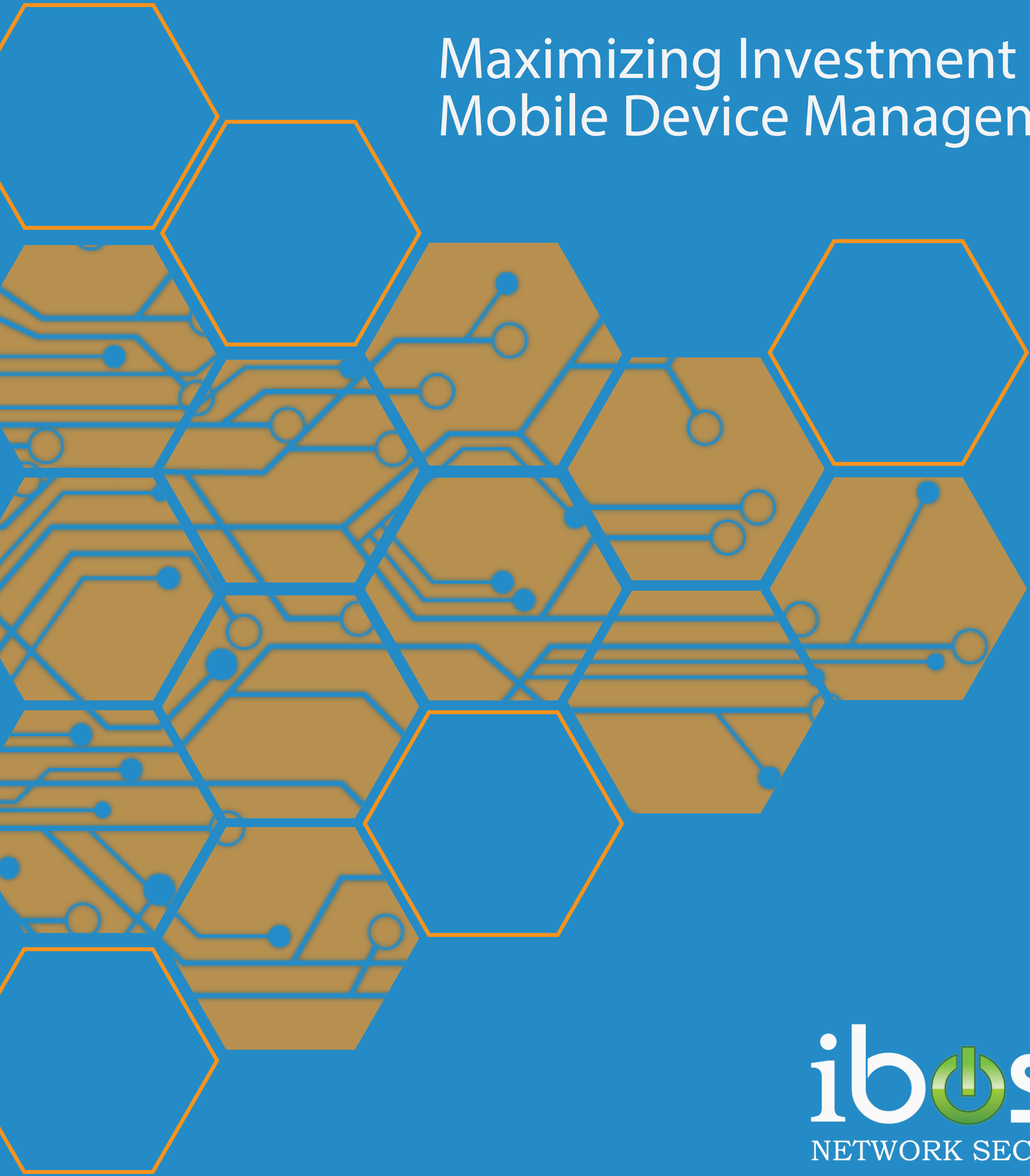
February 2014

Maximizing Investment in Mobile Device Management



iboss™
NETWORK SECURITY

Mobile Devices in Education

There's no question about it — when school districts purchase iPads or other mobile devices for education, their budgets take a big hit. What's perhaps even more brutal to their bottom lines is that they must immediately, often unexpectedly purchase Mobile Device Management (MDM) solutions to both manage these new devices and address the explosive popularity of Bring Your Own Device (BYOD) technologies in classrooms and on campuses nationwide.

Understanding the Costs

When districts don't accurately grasp the considerations and costs of MDM or BYOD for schools, the process of picking the best solution quickly becomes complex, risky and potentially pricey. For example, purchasing a cookie-cutter Internet security filter and MDM product might address general management and threat issues, but it will never be specifically tailored to tackle the unique MDM challenges that the education industry faces. Consequently, districts are unknowingly misspending their dollars, getting less in return for their investment, and compromising network security and function. The latter, of course, can equate to thousands of dollars in emergency computer and network system repairs.

Districts could also be losing out on potential savings, too. Understandably worried about the dangers that unsecured BYOD might pose to school networks or MDM systems, districts may discourage students and teachers from using personal devices. In response, they delegate more dollars toward brand-new, school-supplied devices for staff, students, admin, etc. to use.

Obviously, it's possible to save money by encouraging more BYOD for education. But, importantly, districts must still support that strategy with an all-inclusive system that provides web filtering for education, application firewall security, and reporting/threat solutions.

Addressing the Momentum of "Mobile"

Meanwhile, the need to address this issue keeps growing, considering a recent Frost & Sullivan report estimated that mobile devices will overtake desktop computers by 2017. To keep up to date with the move to 1:1 technologies, districts must research all they can about BYOD for education and MDM. Why? Because unlike corporations, which can reprimand and even fire employees for wrongful use of their technologies and systems, schools can't "fire" their students. The onus is on the districts — in part due to law that protects students and in part due to their need to protect the security of the functionality of their own systems — to ensure their systems are as seamlessly functional, risk-free and secure as possible.

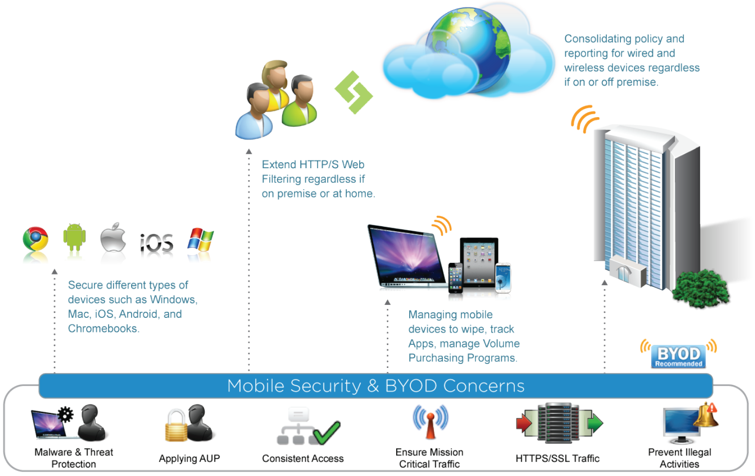
Researching the Considerations

When it comes time to purchasing iPads, Androids and other mobile devices (or saving money through more BYOD for schools), the following considerations can help districts explore and find the best solution for their needs:

- **CIPA compliance.** District-owned devices must meet the requirements of the Children's Internet Protection Act (CIPA) both on and off premise. Not all MDM software products/ programs are created equal — many lack the ability to meet CIPA demands and other highly specific education needs.

• **Integration with existing security.** Districts usually have some level of network security infrastructure, but the software doesn't necessarily provide filtering for today's mobile devices. Districts need to check if an outside web-filtering solution will be required. If so, again, it needs to be CIPA-compliant.

• **Flexible filtering.** A smart web filter provides "flexible filtering," so it can balance the needs of teachers and staff vs. students. This means the ability to establish and offer different user policies based on expected user needs. For example, with flexible filtering, YouTube might be available to all users, however, advertising and inappropriate comments and content gets blocked.


Consolidating policy and reporting for wired and wireless devices regardless if on or off premise.
Extend HTTP/S Web Filtering regardless if on premise or at home.
iOS
Secure different types of devices such as Windows, Mac, iOS, Android, and Chromebooks.
Managing mobile devices to wipe, track Apps, manage Volume Purchasing Programs.
BYOD Recommended
Mobile Security & BYOD Concerns
Malware & Threat Protection
Applying AUP
Consistent Access
Ensure Mission Critical Traffic
HTTPS/SSL Traffic
Prevent Illegal Activities

• **Controlling site accessibility.** Similar to parental controls, schools would regulate which websites users can open in full, so perhaps allowing everyone to access twitter.com/abcschools but preventing access to twitter.com.

• **Mobile application downloads.** Districts need to ask how they'll manage APPs when they're downloaded from stores onto their mobile devices. Will the APP store remain open to all users, enabling students to download APPs? What about those that are rated 17+? How about games? Savvy MDM includes management options for what, if anything, gets downloaded and when.

• **Electronic purchases.** With a growing number of people downloading e-books and other e-materials to mobile devices, districts need to consider how such purchases will be allowed if at all. A tracking system, monitoring which mobile device has what books or licenses downloaded, can be used to prevent thousands of wasted dollars (e.g., license fees or book costs) should the device be wiped or stolen.

• **Tracking devices.** If a mobile device is to remain on campus at all times, what security measures are in place if it's suddenly lost or stolen? Recovery of the item may or may not be possible, but having a way to track the device's whereabouts and/or wipe its contents provides critical peace of mind.

• **Tampered devices.** When a student accidentally locks a password-protected device and prevents another student from using it, there needs to be: 1) a remediation process in place so it can be opened quickly, e.g., while in class; and 2) MDM tools to prevent this from happening in the first place.

• **Device-sharing solutions.** It's become increasingly common for students to share school-owned devices for projects and assignments. So, for example, if multiple students are sharing an iPad for a team project or lab, it's important to have a flexible, yet secure MDM system that applies policy based on each, current user.

• **Content-sharing solutions.** Teachers must be able to easily push documents, such as homework assignments, announcements, grades, and links to students located both on and off campus. Whether kids are staying home sick or studying as long-distance learners, content-sharing solutions enable a fluid learning experience.

• **Interactivity.** Today's MDM solutions should eliminate unnecessary stress, ideally offering a dashboard feature to enable and foster smooth, speedy communication among teachers, students and parents.

- **Identifying & tracking BYOD users.** To maximize the benefits of technology in the classroom, it's helpful to identify users according to the type of user (teacher, student, staff, admin, etc.) and apply policies based on these different user types as opposed to applying a generic user policy to everyone who is utilizing the system.

Finding a Solution

Whether going down the path of purchasing school-supplied mobile devices, encouraging students and teachers to bring their own iPads and Androids to school, or supporting a hybrid approach to MDM, it's critical for districts to get a good grasp of what's involved to make it a success. At the very least, schools need a dependable, flexible Internet content filtering and security solution that addresses the specific demands and requirements that today's education system must meet. They also need to arm themselves with an understanding about MDM, stay abreast of updates and expect new developments.

Why? Because as the world goes more mobile, so, too, are schools being forced to embrace the ever-evolving technologies. Having network security and filtering systems that grow and easily sync with the "device of the day" will maximize the value of the investment. It's possible that the costs and considerations associated with this investment may be significant over time, particularly at the start. But if districts fail to do their MDM homework, or overlook the lasting value of an education-based Internet content filtering and security system upfront, there could be an even bigger price to pay in the near future.

For more information about secure MDM for K-12 or higher education, visit iboss Network Security at: **www.iboss.com.**

iboss Network Security Products

Layer 7 Web Security

- Web Security
- Cloud Web Security
- Threat & Event Console

Web Security Extension Modules

- IPS & Behavioral Data Protection
- Intelligent Bandwidth Management
- Mobile Security
- Mobile Device & Application Management

About iboss Network Security

iboss Network Security engineers highly scalable Web security solutions providing layer 7 defense across HTTP, SSL, threat and applications securing mobile devices on or off network. iboss enables organizations to safely adapt social media, SaaS, and mobile devices while expanding access to technology. By incorporating unmatched network traffic visibility, organizations are able to identify high-risk user behavior and the Shadow IT to create more actionable policies. Visit www.iboss.com.