Box Elder School District Web Security and Filtering

Box Elder School District has deployed an enterprise web security and filtering solution, iboss, to protect the students and staff.

iboss is recommended and supported by UEN (The Utah Education Network). In addition, it is deployed in the majority of Utah School Districts.

iboss is not just a k-12 Education Product, it is deployed by over 4000 entities, in the business, finance and higher education sectors.

Web Security and Filtering

iboss offers comprehensive, content-aware Web Security and Filtering features that protect your network from advanced threats, while enabling granular control over Web access. Leveraging total port visibility, and stream-based, inline technology, iboss enforces corporate AUP and regulatory compliance requirements, while protecting the network from advanced threats in real time.

Comprehensive Dynamic URL Database

The iboss URL database covers millions of sites and is compiled using automation tools as well as human review. The database is continuously and dynamically updated and new sites are added as soon as they become available on the Internet.

Zero-Day Threat Protection

iboss combines global cloud services, the Kaspersky industry-leading signature and heuristic database and local network database access to identify and block threats at the gateway, before they can reach your internal servers. Rather than the daily or weekly updates you get from standard solutions, iboss updates your database in real time, to stop new and emerging threats and ensure continuous protection against malware, viruses, and infected sites.

Granular Filtering Controls

iboss provides granular controls that allow you to configure your Web access to fit your organization's precise requirements.

Social Media Controls – iboss content-aware flexibility means you can allow business-critical Internet tools, without having to block sites completely. iboss granularity allows you to make a site available to a specific directory group – HR vs. Sales, for instance – or you can restrict parts of a site, such as allowing access to Facebook, but restricting posting. This approach improves the end-user experience while assuring accurate enforcement of organization security policies.

Port Access Management – iboss enables you to restrict ports or open them based on local or directory group memberships. This allows you to give access where it's necessary, so users continue mission-critical processes uninterrupted, while restricting others, who don't require access. This adds an important layer of security to your network, and increases user satisfaction.

Keyword Filtering – iboss keyword defense identifies any communications within legitimate sites that pose a threat or violate the organization's policies. Predefined keyword lists are included and custom lists can be imported. Additionally, triggers can be set to immediately email administrators upon detection of high risk or suspicious words.
Domain and File Extension Restrictions – iboss gives you the ability to block access by domain extension, based on directory or local-group membership. In addition, iboss allows you to restrict access to file extensions and executables to prevent accidental downloading of damaging threats, while ensuring that valid file extensions continue to function.
SafeSearch Enforcement – This features applies strict safe search enforcement on Google, Bing and Yahoo search engines, including image searching. With this option enabled, the safe-search preference is automatically set to "strict", preventing any attempts to circumvent it.
Google Services Support – Services such as Google Images and Translation are cached, so organizations must rely on Google SafeSearch, forcing some of them to restrict access completely. iboss technology solves this problem by scanning content, applying your AUP and stripping restricted content directly from the search results, which SafeSearch can't provide.

Question & Answers

Q: Are there different settings for different grade levels?

A: No. The settings are universal for students.

Q: How does the district handle Social Media websites such as Twitter, Facebook, Instagram, etc.

A: Currently, for the protection of the students, and to keep students focused on school work, social media on the district network is blocked by the filter for students.

Q: How does the district handle image searches?

A: Currently image searches are redirected to Clean Image Search provided by our internet filter provider iboss. This provides clean search results for students.

Q: What about web hosting sites such as Weebly, Wixom & others?

A: All hosting services have the potential of containing inappropriate content and are considered "Private" websites. The district currently blocks all private websites. They are allowed on a case by case basis if it is determined by administrators that the site meets the educational needs of our students.

Q: What about mobile devices, are they protected?

A: Yes. All mobile devices are enrolled in multiple device management systems (MDM and Chrome Management) that provide control for the school district. Students using mobile devices are subject to the same filtering rules as "hard wired" desktop computers.

Q: Are there other safeguards in place?

A: Yes. Many of our schools utilize LAN school which allows a teacher in a computer lab setting to monitor the activities of students. A Teacher/Lab Manager can view that the students are seeing on their monitor at any time.

Q: How does the district educate students on being safe digital citizens?

A: Our elementary schools currently use the "NetSafe Utah" http://www.netsafeutah.org/ curriculum which educates students on internet safety.

Q: What happens when students or other access inappropriate content?

A: It depends. If it was intentional, it is considered a violation of the AUP (Acceptable Use Policy) and students will be disciplined which may include, suspension of computer access. Parents are notified of violations. If it was unintentional, the BESD IT staff immediately investigates to determine how to block future access. Depending on the severity of the material, parents may be contacted. All who use the district network are subject to the district AUP policies 3085 & 4177. Violations by adults are referred to the district personnel office for appropriate corrective action.

BEMS Responsibilities - Digital Technology

What devices are being used and how are the classes using them?

- Devices: chromebooks, mini iPads, computer labs, some personal electronics
- Uses: access online books and curriculum, research, complete assignments, additional information and resources

What are the main applications, programs, and sites being used in different classes, grade levels and subject areas?

- My Access
- Digits
- L.A. Curriculum
- Science Textbook
- Research

What supervision practices are in place when students are online?

- Proximity - movement around the room during student work
- Specific directions and predetermined websites/activities
- BEMS has the ability to see who has logged into specific computers and websites they visited

Are there management tools used to allow teachers to digitally monitor student use or limit access to some applications or sites?

- 2 CTE labs have ability to control all computers from the teacher computer
- District software and precautions in place to limit access to inappropriate websites

What are the school rules when inappropriate information appears for students, staff and parents? Are there safe reporting procedures for students, staff, and parents so that reporting is safe and encouraged when it happens?

- Procedure is close sites, web browser, or computer immediately and to report incident to teacher as soon as it happens.
- No specific place or way, but reporting to teacher or administrator will allow BEMS personnel to submit request to District Instructional Technology (IT) Team to restrict access to that link or website.

How does the school balance access and safety appropriate for the 8th and 9th graders?

- With the help of the District IT Team and good practices, BEMS strives to allow students an opportunity to explore, discover and learn with technology by limiting access to inappropriate sites.
- Teachers also monitor and check student access during class and check websites and content before instruction ever takes place.
- The District requires that each student signs a Computer Use Policy, outlining what is appropriate and not appropriate on district computers.

What does the administration see as important opportunities for our students to relate to constructive, proactive technology?

- Some of these important opportunities is accessing grade/class -specific material in a variety of mediums, researching content, discovering questions and answers to questions, using technology as a tool to enhance learning, and allowing technology to be a piece of their learning, exploring, and sharing of knowledge.

What does the administration see as their greatest threats for our students?

- Cyber-bullying – social media

- Technology assumptions - requiring so much online activities that may put extra pressure on families with multiple students needing access simultaneously

What are the policies in place for devices brought from home - personal electronic devices?

- School Board Policy 4177 - I may access the district's WLAN (where it exists) with a personal computer device including smartphone, iPad, iPod, laptop, or tablet for educational purposes if sponsored by a teacher and in accordance with Policy 5305. Violation of any provision of this policy will result in a loss of that privilege
- Currently at BEMS students are not able to access the school wifi

BEMS Handbook:

- **Bullying, Harassment, Cyber bullying, Hazing, Retaliation, Anonymous Reporting and False Reporting:** Bullying, cyber bullying, harassment, and hazing of students and employees are against federal, state and local policy, and are not tolerated by BEMS. We are committed to providing all students with a safe and civil school environment in which all members of the school community are treated with dignity and respect.
- **BEMS considers bullying to be aggressive behavior that:** is intended to cause distress and harm; exists in a relationship in which there is an imbalance of power and strength; and is repeated over time.
- **COMPUTERS/TECHNOLOGY:** At Box Elder Middle School, I will have access to state of the art technology. Prior to using any computers or digital devices in the classrooms, media center, or labs, I will review the Box Elder School District Computer Use Policy with my parents/guardian and return a signed copy to my prime time teacher. I will not bring any personal disks from home.
- **COMPUTER USE POLICY:** Each student each year will sign and return to the main office the computer use form as found at the following district website: http://www.besd.net/district/policies.php?pgid=4

What does the administration see as the greatest threats for our students on the internet or online?

- Lack of parent supervision
    - Parents need to be involved, know passwords to accounts, follow accounts, hold their children accountable and responsible for what is said and posted

Explanation of training provided:

To the students about digital citizenship and safe use of technology?

- In all technology classes they review these rules and safeguards.
- Teachers review rules periodically as they use digital devices in their classrooms and the school labs.

To parents and guardians about how to discuss and support digital citizenship and safe technology use with their children and how to report inappropriate content?

-
-
-