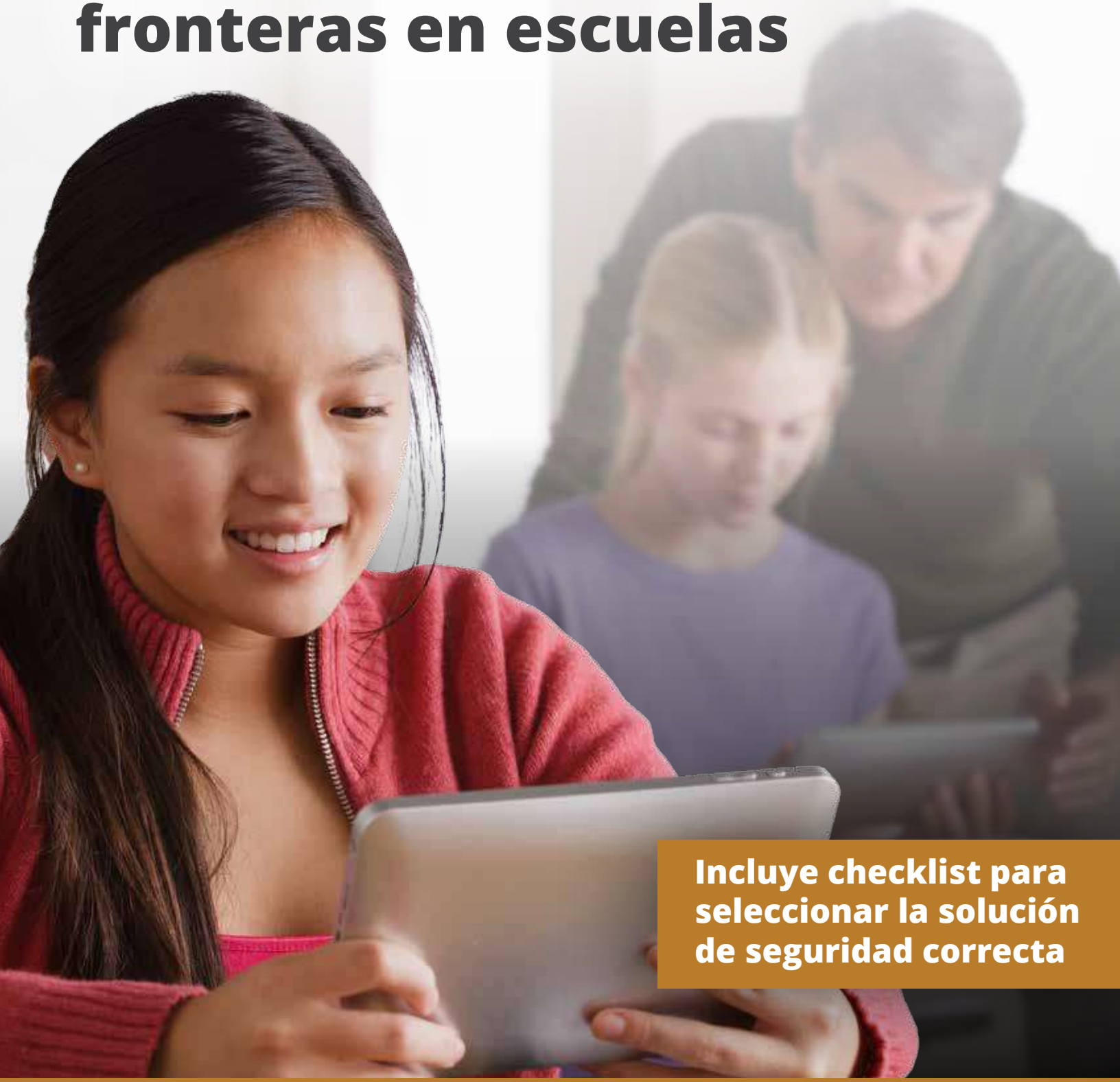
iboss NETWORK SECURITY

Móviles en Salones de Clase:

Como asegurar las redes sin fronteras en escuelas



Incluye checklist para seleccionar la solución de seguridad correcta

Dispositivos Móviles en la Educación

Apple presume que cerca de 10 millones de iPads se encontraban en las manos de estudiantes de todo el mundo durante el 2013, y que ese número esperaba aumentar sustancialmente en los próximos años. Otras marcas de tablets también se encuentran aumentando su presencia en las escuelas mientras que los educadores han sido rápidos en descubrir que los recursos educativos en el Internet pueden aumentar la experiencia de aprendizaje y son amigables con el presupuesto. Los libros de texto digitales custan alrededor de la mitad de costo por estudiante que los libros impresos, y con los apretados presupuestos escolares, la tecnología móvil en escuelas, incluyendo el bring-your-own-device (BYOD), continuara expandiéndose. Un reporte analísta reciente de la industria estima que los dispositivos móviles estarán sobrepasando las computadores de escritorio para el 2017.

Mientras que existen mucho beneficios asociados con los dispositivos móviles en los salones de clases, la habilitación del móvil en las escuelas presenta nuevos retos para los profesionales de seguridad de redes encargados de salvaguardar a los estudiantes, proteger la red de la escuela, mantener el cumplimiento de regulaciones como la Children's Internet Protection Act (CIPA), políticas de uso aceptable y asegurando la disponibilidad de la red.

Dispositivos propios de la Escuela vs. BYOD

Muchas escuelas han adoptado la iniciativa 1:1 proporcionando iPads y otros dispositivos móviles a los estudiantes en escuelas K-12. Otras escuelas están permitiendo programas bring-your-own-device (BYOD) en donde los estudiantes llevan sus dispositivos móviles y se conectan a la red de la escuela. Cada uno de estos programas presentan ventajas y retos para las escuelas:

- Ofrecer dispositivos móviles a los estudiantes significa que las escuelas deben de asegurar que el dispositivo se encuentre en cumplimiento con CIPA al asegurar el acceso a la web en el dispositivo. Además, las tablets con iOS y Androids también pueden llegar a requerir un MDM para Administración de Dispositivos Móviles para administrar las aplicaciones y periféricos en el mismo dispositivo.

- Los dispositivos propios de la escuela crean un estatus igual entre los estudiantes ya que se encuentran con la misma tecnología - también es más fácil para los maestros administrar las tareas para los estudiantes bajo la misma plataforma.

- Los dispositivos propios de la escuelas son más fáciles de asegurar, debido a que se tiene la capacidad de instalar software en los dispositivos para administrarlos, pero el permitir el BYOD ofrece el ahorro de proveer una tablet para cada estudiante.

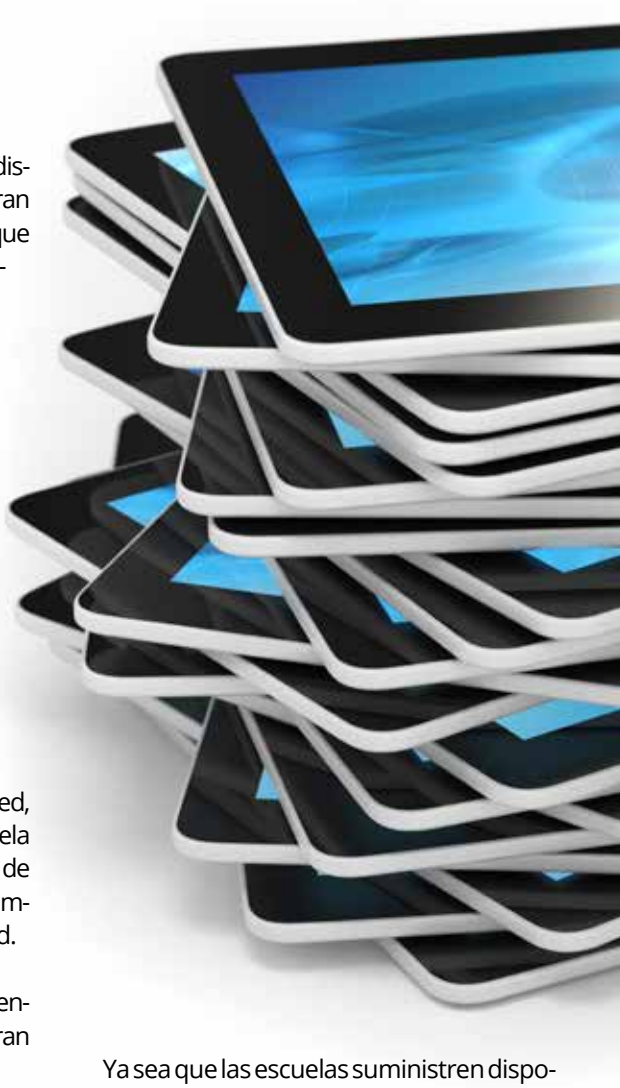
- El BYOD ahorra el costo de comprar dispositivos y los usuarios se encuentran más comodos con los dispositivos que les pertenecen y se encuentran acostumbrados en usar, pero el BYOD puede introducir nuevas amenazas a la red de la escuela debido a que los estudiantes sin saberlo pueden llevar un dispositivo ya infectado a la red.

- El BYOD incluye multiples plataformas y aplicaciones que generan retos de soporte así como la dificultad para identificar los eventos de actividad web por nombre del usuario en el directorio vs. número IP.

- Con más dispositivos móviles en la red, ya sea que pertenezcan a la escuela o BYOD, se aumenta la demanda de ancho de banda y puede llegar a comprometerse la disponibilidad de la red.

- Controlar los dispositivos pertenecientes a la escuela cuando se encuentran fuera de la red puede ser difícil.

- Administrar las actividades de usuarios BYOD incluye consideraciones a la privacidad.



Ya sea que las escuelas suministren dispositivos móviles propios a estudiantes y personal, permita el BYOD o permita ambos, los dispositivos móviles presentan riesgos y retos tanto para la administradores de la escuelas, como para el personal de TI.

Enfrentando las Amenazas y Riesgos Móviles

Desafortunadamente, así como la tecnología móvil continúa evolucionando, así también las tácticas de los cibercriminales dedicados a explotar las debilidades. Las escuelas no se encuentran inmunes a las amenazas avanzadas persistentes (APTs) y explotaciones de día-cero que se encuentran en aumento apuntando hacia los usuarios móviles. Sin embargo, muchos vendedores de seguridad se encuentran tratando de asegurar las redes sin fronteras de las escuelas con tecnología que fue desarrollada antes de que los móviles en los salones de clases existieran. Otros obstaculos para asegurar a los usuatios móviles en escuelas son:

- El crecimiento de los dispositivos móviles inalámbricos se encuentra igualado por la inteligencia de los mismos, haciéndolos capaces de soportar el aumento de sofisticadas aplicaciones que generan más riesgos para la TI de la escuela.
- Los sindicatos del cibercrimen contratan hackers con talento e intercambian o venden kits gratis para explotaciones, con tácticas tan creativas como las soluciones que tratan de frustar.
- El aumento en el número de aplicaciones proxy tal como Ultrasurf, Tor y otras fueron diseñadas para habilitar la navegación anónima, permitiendo a los estudiantes circunnavegar la solución de seguridad Web de la escuela.
- Las escuelas necesitan considerar la amenaza a la pérdida de datos así como proteger el acceso al Internet de los estudiantes. Esto es por lo que más allá del CIPA, las escuelas requieren asegurar que la información de salud de estudiantes y personal se encuentra bajo las regulaciones de HIPAA así como el cumplimiento con FERPA (Family Educational Rights and Privacy Act). El cumplimiento de estas regulaciones demanda la vigilancia sobre los datos que dejan la red de la escuela y el malware roba-datos entrando.
- Asegurar los dispositivos móviles puede ser costoso y una carga al ajustado presupuesto de las escuelas. La escasez de soluciones integradas tiene a muchos vendedores procurando hacer un upgrade de las soluciones legadas para incluir tecnología que no existía cuando fueron creadas. Como resultado, los vendedores tratan de integrar el MDM de terceros, los cuales pueden crear agujeros profundos de seguridad.

El Móvil y el Ciberbullying

Con más estudiantes móviles accesando a la red de la escuela, no es sorpresa que también se encuentren accesando a las aplicaciones de redes sociales más seguido vía los dispositivos móviles. De acuerdo a Pew Research, el 74% de los estudiantes entre los 12-17 años son usuarios móviles del Internet que tuvieron acceso a la Web vía teléfonos celulares y tablets, y el 81% accesando a sitios de redes sociales. Estudios recientes muestran que el ciber-bullying en las escuelas K-12 se encuentra rampante, el 87% de estudiantes de nivel-medio reportaron ser testigos del ciber-bullying en el último año.

Previo al advenimiento de los dispositivos móviles, los incidentes de bullying ocurrían en persona y los perpetradores podían ser identificados. La disponibilidad de las comunicaciones móviles acoplada con las numerosas y populares plataformas de redes sociales se han acomodado en una era de ciber-bullying en donde el intimidador puede permanecer anónimo para la víctima. Desafortunadamente, el daño a las víctimas sigue siendo el mismo

y las escuelas se pueden considerar culpables si las ofensas ocurren durante el horario escolar o vía la red de la escuela, o hasta fuera de la misma si emplea dispositivos proporcionados por la escuela. Hay muchos casos de escuelas demandadas por permitir que los estudiantes sean acosados con el ciber-bullying, incluyendo:

- Williamson County Schools en Tennessee fue demandada por $1.1 millones de dólares por padres que reclamaban que el distrito escolar no hacía lo suficiente para proteger a sus hijos del ciber-bullying en Facebook.
- El Distrito Escolar de Estacada en Oregon fue demandada porque el video de un estudiante cambiándose en los vestidores fue publicado en sitios de redes sociales.
- El personal de una escuela en Luousiana fue demandado por el suicidio de un estudiante que fue acosado por sus compañeros.

Retos de Iniciativas1:1 y Soporte BYOD

Ya sea que su escuela o distrito seleccione adoptar una iniciativa1:1, soportar el BYOD o ambos, existen riesgos de seguridad asociados con ambos programas. Aquí presentamos una comparativa de los retos que cada uno presenta.

1:1 Iniciativas	BYOD
Proporcionar iPads o cualquier otra tablet a cada estudiante puede ser una carga pesada para los ajustados presupuestos en escuelas y con la tecnología moviéndose tan rápido, puede ser difícil costear las actualizaciones tecnológicas cuando estas se requieran.	Mientras que se permiten los dispositivos móviles personales en su red para liberar el presupuesto de la escuela, estos pueden introducir nuevas amenazas a la red. También existen cuestiones de privacidad cuando se trata de usuarios BYOD.
El tener a los estudiantes y maestros utilizando los mismos dispositivos requiere de la capacitación para aquellos que no están familiarizados con la tecnología seleccionada - agregando tiempo y costos.	Los anonimizadores y servicios para compartir archivos, permiten a los estudiantes BYOD con conocimientos prácticos circunnavegar la seguridad Web de la escuela, son campo fértil para los ciber-criminales que buscan explotar vulnerabilidades.
Mientras que los estudiantes BYOD son responsables del mantenimiento y seguridad de sus propios dispositivos, la escuela estará aceptando mayor responsabilidad legal por los dispositivos que proporcionan.	La variedad de sistemas operativos en el BYOD hace que su aseguramiento sea más complejo. También, los usuarios que fallan al realizar la actualizaciones oportundas pueden contener bugs de versiones previas.
Para asegurar el acceso Web de estudiantes y personal y proteger los dispositivos pertenecientes a la escuela se requiere de un software MDM, lo cual puede agregar un costo considerable a su programa 1:1.	La erosión en el rendimiento de la red puede ocurrir cuando multiples dispositivos móviles se encuentran consumiendo el ancho de banda. Estos impredecibles y aumentados niveles de demanda pueden interferir con procesos importantes tal como los exámenes en linea.

Checklist de su próxima Solución de Seguridad Móvil

Ya sea que su escuela adopte un programa 1:1, permita el BYOD o ambos, dependerá de su escuela o distrito asegurar la seguridad de usuarios y dispositivos.La siguiente lista puede servir como una guía de capacidades cruciales que incluir mientras que refina su estrategia de seguridad móvil y evalúa soluciones de seguridad:

Soporta todos los requerimientos para el cumplimiento de regulaciones: los esrudiantes y personal en escuelas con dispositivos móviles propios debe de encontrarse en cumplimiento con los requerimientos de CIPA y otras normas para dentro y fuera de premisas. Los usuarios en dispositivos propios-privados también deben de cumplir si se encuentran accesando a través de la red inalámbrica de la escuela. Asegurese que la seguridad móvil que seleccione le ofrezca la habilidad para ejecutar cualquier cumplimiento de regulación requerida. Mantengase consciente que las soluciones MDM estándares pueden carecer de las capacidades requeridas para soportar con precisión el cumplimiento de regulaciones de las escuelas.

Soporta multiples plataformas: Para escuelas que habilitan programas BYOD, es importante tener soluciones de seguridad Web y Móvil que se puedan integrar a través de cualquier plataforma. Con una variedad de dispositivos móviles disponibles, si solución de seguridad no es lo suficientemente flexible para soportar multiples plataformas, usted puede colocar en riesgo los esfuerzos para el cumplimiento de regulaciones.

Ofrece la protección de amenazas avanzadas a través de todos los dispositivos móviles: La mayoría de las escuelas tiene soluciones para la seguridad Web / filtrado Web, pero muchas de ellas fueron desarrolladas antes de que las conexiones móviles existieran. Asegúrese que su solución de seguridad no solo prevenga de amenazas avanzadas, incluyendo las que utilizan el tráfico SSL/HTTPS, sino que también ofrezcan la protección granular a través de todos los dispositivos móviles ya sea que pertenezcan a la escuela o BYOD. Con las amenazas móviles aumentando cada día, usted necesita una solución que expanda la proteción a todos sus usuarios móviles o estará dejando vulnerable a su escuela a un amplio rango de malware perjudicial y otras explotaciones.

Integración con soluciones de seguridad existentes: Debido a que virtualmente todas las escuelas cuantan con soluciones de seguridad Web en sitio, el encontrar soluciones para la seguridad móvil que se integren fácilmente con el software existente es importante. Asegurese de no solo revisar las funcionalidades del MDM que cumplan con los requerimientos de su escuela, sino también que comprendan cuales son los pasos para integrar un MDM dentro de su solución de seguridad Web existente. En muchos casos, la integración puede requerir la reconfiguración de su firewall así como la configuración de proxies lo cual puede ser costoso y consumidor de tiempo.

Ofrece la ejecución granular de políticas: Es importante para las escuelas el poder reforzar el uso de políticas de uso de la Web a través de diferentes audiencias, por ejemplo, aplicar políticas a profesores / personal administrativo vs estudiantes, o estudiantes jovenes vs estudiantes más gandes, etc. En el caso de los dispositivos que pertenecen a la escuela, en donde las iPads o tablets pueden cambiar de manos durante el día, la habilidad para determinar con precisión quien se encuentra utilizando el dispositivo en un momento en específico es importante.

Atender el uso de ancho de banda: Con más dispositivos móviles accesando a la red de la escuela, usted necesita una solución de seguridad móvil que pueda asegurar la disponibilidad de la red durante las horas pico. Esto es particularmente crítico para las escuelas donde las pruebas son aplicadas y la disponibilidad de la red es primordial.

Ofrece el acceso inteligente a las redes sociales: Las reglas actualizadas de CIPA efectivas a partir de Julio, 2012, requieren que las escuelas enseñen a los niños a comportarse apropiadamente en linea dentro de las redes sociales y salones de charla. Asegurese de seleccionar una solución de seguridad que ofrezca el escaneo consciente del contenido y el control granular de las redes sociales para que pueda ponerla a la disposición de los esudiantes en un ambiente seguro. Por ejemplo el permitir el acceso a secciones apropiadas dentro de un sitio mientras que bloquea los comentarios. En otro escenario, sería importante ser capaz de bloquear el acceso a twitter.com, mientras que permite el contenido de twitter.com/abcschools.

Control de descarga de aplicaciones móviles: Con miles de aplicaciones móviles disponibles, las escuelas necesitan tener una solución MDM que pueda desplegar las aplicaciones que los estudiantes y el personal necesitan, y bloquear el acceso a las aplicaciones que no se encuentran relacionadas con la escuela o la edad apropiada. ¿La App Store va a estar abierta para que los estudiantes descarguen lo que quieran? Seleccione una solución que le ofrezca el control sobre que apps son descargadas y cuando, y pueda desplegar aplicaciones importantes o personalizadas a los grupos o individuos correctos.

Rastreo de dispositivos pérdidos o robados: Las escuelas deben de considerar la posibilidad de que los dispositivos que ofrece a estudiantes y personal pueda ser robado o extraviado. ¿Qué medida de seguridad tendrá desplegada para hacer frente a esta posibilidad? Aunque la recuperación puede que no sea posible, tener la posibilidad de rastrear la localización del dispositivo y/o limpiar su contenido ofrece la tranquilidad mental.

Rastreo de compras electrónicas: Si sus estudiantes y personal se encuentran descargando e-books autorizados y otro tipo de contenido en los dispositivos pertenecientes a la escuela, usted va a requerir una solución MDM que pueda llevar el registro de las licencias legítimas para la descarga del material para estudiantes y maestros. Un sistema de rastreo para el monitoreo y rastreo de las compras y licencias que pueda prevenir la pérdida monetaria si el dispositivo es borrado o robado.

Mitiga la manipulación: Los dispositivos pertenecientes a la escuela pueden bloquearse por accidente o intencionalmente, impidiendo que otros usuarios los utilicen. Asegurese de tener una solución MDM con todas las herramientas para remediar este problema lo más rapido posible si llega a suceder, o mejor aún, evitar que suceda en primer lugar.

Aplicación precisa de políticas en dispositivos compartidos: Los estudiantes pueden estar compartiendo los dispositivos pertenecientes a la escuela o trabajar en grupos en donde los dispositivos son compartidos. Es por eso que es importante tener una solución MDM que ofrezca la integración con la seguridad Web basada en políticas. Seleccione una solución que le permita ejecutar con precisión las políticas sin importar quien se encuentre utilizando sus dispositivos móviles.

Habilita compartir el contenido: Los maestros deben de tener la habilidad para empujar documentos, tal como tareas de asignaturas, anuncios, calificaciones, y ligas para los estudiantes que se encuentren dentro y fuera del campus. Ya sea que los niños se encuentren enfermos en el hogar o estudiando a larga-distancia, las soluciones que permiten compartir contenido ofrecen una experiencia de aprendizaje más fluída.

Ofrece una interfase intuitiva: Busque una solución MDM integrada que ofrezca características de fácil uso y consola intuitiva que ofrezca la rápida comunicación entre maestros, estudiantes y padres cuando sea requerido. No existe una razón para agregar complejidad al MDM con una solución que es difícil y lenta de usar.

Identifica y rastrea los usuarios BYOD: Tal y como rastrea los usuarios móviles en los dispositivos propios de la escuela, si usted permite el BYOD en la red de la escuela, usted va a querer la misma habilidad para rastrear su actividad Web, ya sean estudiantes, maestros o personal. Mientras que algunas soluciones ofrecen aplicar políticas de uso genéricas para todos los usaurios BYOD, busque una que permita rastrear a individuos y ofrecer la ejecución precisa de políticas.

iboss Seguridad Web y Móvil:

iboss ofrece soluciones para la seguridad Web y Móvil integradas que son fáciles de desplegar y administrar para ofrecer el control granular con un conjunto rico de características que puede soportar a todos sus usuarios, y reforzar el cumplimiento de regulaciones ya sea que los estudiantes y el personal se encuentren utilizando dispositivos propios de la escuela o personales. Las características más importantes de la seguridad móvil de iboss incluyen:

MDM y seguridad móvil en una sola solución – MobileEther

MDM y seguridad Web con iboss MobileEther – Solo iboss ofrece la administración de dispositivos móviles (MDM) con características completas y la Seguridad Web Integrada para asegurar ambos dispositivos y el acceso Web de la escuela en una sola solución. En una interfase, las escuelas pueden localizar los dispositivos, limpiar los dispositivos perdidos o robados, y hasta deshabilitar funciones tal como las camaras. Las alertas enviadas por email ofrecen la vista a profundidad de los eventos definidos por el administrador, tal como cuando un dispositivo deja la red, una aplicación no aprobada es instalada, o cuando una violación al acceso web ocurre. Dieciocho diferentes disparadores que pueden ser personalizados para mantenerlo informado de toda la actividad del usuario, ya sea que se encuentren dentro o fuera de la red. Si usted ya tiene una solución MDM, la seguridad móvil de iboss puede ser integrada con el MobileEther deshabilitado.

Controles para redes sociales – MobileEther permite a las escuelas ofrecer el acceso flexible a las redes sociales basándose en la membresía de un grupo del directorio. Además, los controles granulares le permiten tener un conjunto de políticas para cada usuario de las redes sociales incluyendo restricciones tal como 'No Posting', 'Juegos' o 'Cargar Fotos' a sitios de redes sociales. Esto le permite habilitar las redes sociales mientras que cumple con CIPA y otras regulaciones.

Administración de aplicaciones – Asegure el control granular de apps con la habilidad de empujar aplicaciones personalizadas, actualizar contenido, restringir o permitirel acceso a la tienda de apps y más. Con el Filtrado de la App Store único de MobileEther, los administradores pueden permitir el acceso a solo las categorías de apliaciones permitidas y clasificadas por edad que los usuarios pueden buscar e instalar por su cuenta.

Enrolamiento sencillo de estudiantes y personal – Enrolamiento en el aire rápido y fácil le permite comenzar en solo minutos, mientras que se encuentre dentro o fuera de premisas, sin requerir de Apple Configurator. Además, el soporte al Programa de Enrolamiento para dispositivos de Apple le permiten enrolar automáticamente los dispositivos a MobileEther sin la interacción del usuario.

Integración completa con directorios y autenticación – Simplifica la integración al obligar los dispositivos a los servicios existentes del directorio incluyendo el Directorio Activo, eDirectory, Open Directory y LDAP. Las políticas para el acceso Web y los perfiles de los dispositivos móviles se basan el los perfiles del directorio y se consolidan a través de una interfase de administración central, la cual simplifica la instalación, administración y mantenimiento.

Consciente del contenido dinámico y reportes – La Seguridad Móvil se encuentra completamente integrada con la Consola de Reportes de Amenazas y Eventos de iboss para ofrecer la visibilidad del contenido dinámico a través de todas las acciones, se encuentren restringidas o no, en tiempo real en cualquier dispositivo. Detecte al instante la actividad sospechosa de dispositivos móviles y reciba alertas. La integración racionalizada con los servicios del directorio permiten agregar reportes a través de todos los usuarios ya sea se encuentren dentro o fuera de premisas.

Ejecución precisa de políticas en dispositivos compartidos – Los usuarios autentificados se encuentran obligados via la integración a su perfil por grupo o individual pero MobileEther puede cambiar la configuración de los dispositivos dinámicamente incluyendo las reglas de acceso al Internet, perfiles del dispositivo, y el acceso a la tienda de apps basado en el usuario en específico con acceso al dispositivo. Esta es una capacidad esencial en ambientes compartidos tal como los salones de clase, librerías o laboratorios, en donde un solo dispositivo puede tener diferentes usuarios.

Contenido Compartido (Lockbox) – iboss permite a los administrados y maestros compartir contenido fácilmente con estudiantes incluyendo documentos, imágenes, audio, video, bookmarks, anuncios, o aplicaciones compartidas. Al utilizar el Lockbox para Compartir Contenido, los maestros pueden crear grupos compartidos basados en sus clases y estudiantes, ofreciendo a los estudiantes el acceso a valiosas herramientas de aprendizaje y aumentando la productividad en los salones de clase.

Administración Delegada – iboss le permite delegar tareas para el control y administración de las políticas para los dispositivos móviles para maestros y administradores, aumentar la eficiencia y facilitando la demanda de recursos de TI.

Grupos de Dispositivos Anidados enJerarquía – Simplifica la administración de políticas al crear arboles de grupos de dispositivos anidados para el despligue de políticas en dispositivos móviles. Crear grupos de políticas, aplicarlas a todos los dispositivos bajo la misma rama.

Seguridad BYOD

La Suite de Seguridad Web de iboss ofrece herramientas BYOD incorporadas que extienden las características líderes de la Seguridad Web a través de todos los ususarios móviles BYOD incluyendo las siguientes funciones:

Portal cautivo para los usuarios BYOD – Administre el BYOD de estudiantes y maestros al obligarlos a los servicios del directorio incluyendo Directorio Activo, eDirectory, Open Directory, y LDAP para conexiones alámbricas e inalámbricas.

Ejecución granular de políticas – Aplicación de políticas por grupo o individual que permite la aplicación precisa de políticas apropiadas para los grupos o individuos tal como maestros, estudiantes mayores, estudiantes menores, etc.

Consciente de la localización – iboss habilita el rastreo consciente de la localización que le permite proteger la privacidad en los dispositivos móviles pertenecientes a usuarios, cuando se encuentran fuera de la red de la escuela. Tan pronto un dispositivo móvil privado deja la red de la escuela, usted necesita asegurar que sus datos privados no están siendo monitoreados y la tecnología BYOD de iboss le ofrece esta seguridad.

Defensa contra amenazas avanzadas – La admistración de iboss BYOD incluye el escaneo y filtrado de amenazas conocidas y desconocidas incluyendo el malware y botnets que pueden invadir las redes de las escuelas. iboss extiende la protección líder de la industria contra amenazas y pérdida de datos para todos los usuarios incluyendo el BYOD.

Cuarentena de usuarios de alto riesgo – Cuando la actividad ilegal o prohibída es detectada en dispositivos móviles privados iboss puede colocar automáticamente en cuarentena de cualquier otra acción al usuario problemático y notificarlo para que el problema sea atendido.

Administración Inteligente del Ancho de Banda – La Suite de Seguridad Web de iboss incluye el perfilado de ancho de banda durante las horas pico, para que pueda optimizar el rendimiento de la red durante las tareas importantes de la escuela como los exámenes en linea .

Acerca de iboss Network Security

iboss Network Security es proveedor líder de soluciones innovadoras para la Seguridad Web, Seguridad Móvil y Amenazas Acanzadas y Protección de Datos. Con el respaldo de tecnología patentada, el enfoque basado en el flujo de iboss ofrece una visibilidad sin paralelos a través de todos los canales de datos inbound/outbound y aplicaciones evasivas de puertos. Con el mejor desencriptamiento del SSL de su calse, controles integrados para el BYOD, MDM proprietario y la administración de ancho de banda incorporada, iboss ofrece la solución más escalable para las complejas redes sin fronteras actuales. Apalancando la protección de amenazas líder y la usabilidad no superada, iboss tiene la confianza de miles de organizaciones y millones de usuarios en todo el mundo.

Visite **www.iboss.com**

WP/MS-EDU-US-5/14

iboss, Inc. (P) 877.742.6832 Sales@iboss.com U.S. HQ 9950 Summers Ridge Rd., Bldg. 160 San Diego, CA 92121