Hoja de datos

Escuelas preparadas para el futuro

Protección de la infraestructura tecnológica para el futuro del aprendizaje

Características principales

- Filtrado web y de contenido completo
- Cumplimiento e informes automatizados
- Administración de tráfico SSL
- Protección de dispositivos móviles
- Protección de tecnologías desactualizadas
- Generación avanzada de informes en tiempo real
- Administración desde un único panel
- Supervisión y ajuste del ancho de banda
- Controles pormenorizados de aplicaciones en la nube y redes sociales
- Soporte técnico EN DIRECTO inigualable

La tecnología está cambiando la educación preescolar, primaria y secundaria, ya que está creando, a un ritmo acelerado, nuevos modelos innovadores de enseñanza y aprendizaje. Como líder de TI, debe proporcionar una seguridad eficaz para toda la tecnología utilizada en las operaciones y los programas educativos de su escuela. Para ello, necesita una solución de puerta de enlace que pueda crecer y cambiar con la rapidez con la que cambian las necesidades de su escuela.

La plataforma Distributed Gateway Platform de iboss redefine la manera en la que se proporciona y se administra la seguridad de la puerta de enlace web. Su revolucionaria arquitectura basada en nodos crea previsibilidad financiera y ofrece un retorno de la inversión inmediato mediante un modelo de suscripción del 100 %. iboss, que se ha implementado en miles de escuelas y protege a millones de alumnos, es el proveedor n.° 1 de puertas de enlace web seguras para el segmento de educación preescolar, primaria y secundaria.

Cómo ayuda la plataforma Distributed Gateway Platform de iboss

iboss simplifica la seguridad de la puerta de enlace web para que los docentes y los administradores se puedan concentrar más en lo que realmente importa: la calidad de la experiencia de enseñanza y aprendizaje que ofrecen. Estos son algunos ejemplos de cómo iboss ayuda a las escuelas a mejorar y optimizar la seguridad de sus programas educativos y operaciones en general.

Cumplimiento de la CIPA. El amplio uso de los dispositivos móviles y los diferentes parámetros de filtrado de contenido para alumnos, docentes y personal han hecho que para las escuelas sea un desafío el cumplimiento de los requisitos de la Ley de Protección de la Infancia en Internet (CIPA). La plataforma Distributed Gateway Platform de iboss elimina este problema y brinda a las escuelas una manera fácil y automatizada de establecer y aplicar el cumplimiento de la CIPA para todo tipo de dispositivos y para los diversos grupos dentro de una comunidad escolar.

Iniciativas 1:1. Al otorgarle a cada alumno un equipo portátil o una tableta, las escuelas deben extender el cumplimiento de la CIPA más allá de sus cuatro paredes (hasta cualquier lugar en el que los alumnos usen esos dispositivos). El redireccionamiento del tráfico en los centros de datos es engorroso y costoso. Por eso, iboss ofrece a las escuelas una forma de proteger en la nube todos los dispositivos móviles, incluidos los dispositivos iOS, Android y Chromebook, al mismo tiempo que elimina los costos y las vulnerabilidades asociadas con el redireccionamiento de los datos.

Habilitación de aprendizaje. El filtrado de contenido no es simple. Las políticas destinadas a bloquear el contenido perjudicial pueden bloquear de manera inadvertida material con valor educativo legítimo y frustrar a los alumnos y a los maestros. Por eso, iboss elimina estos problemas mediante controles de políticas pormenorizados, incluido el descifrado de SSL selectivo, lo cual permite garantizar que se bloqueará el contenido inapropiado y se conservará el contenido educativo útil.

Características principales *Capacidades completas para educación preescolar, primaria y secundaria*

La plataforma Distributed Gateway Platform de iboss incluye muchas funciones de filtrado de contenido, seguridad y administración, que respaldan las iniciativas de aprendizaje digital, dentro y fuera del aula. Las siguientes son características principales que nuestros clientes de educación preescolar, primaria y secundaria consideran valiosas:

Filtrado web y de contenido completo para bloquear el acceso al contenido en línea que es perjudicial u ofensivo.

- Protección basada en secuencias que cubre todos los puertos y protocolos (TCP y UDP).
- Filtrado pormenorizado por categoría y por usuario.
- Alertas en tiempo real basadas en palabras clave y eventos, y otros desencadenadores personalizables.
- Bloqueo de tipo MIME de contenido, bloqueo de extensiones de archivos y bloqueo extensiones de dominios.
- Administración de acceso a puertos.
- Base de datos de URL dinámica en tiempo real.
- Análisis e inspección profundos de archivos basados en proxy.

Cumplimiento y generación de informes automatizados para establecer y aplicar políticas con el fin de garantizar y documentar el cumplimiento de todas las normas del sector aplicables para la privacidad y la protección de datos.

- Tecnología de filtrado de contenido que cumple con la CIPA para alumnos y personal.
- Tecnología que cumple con la HIPAA mediante el Acuerdo de asociados comerciales.

Administración del tráfico SSL para supervisión y administración de la creciente cantidad de tráfico cifrado en las redes de las escuelas, especialmente los intentos de usar SSL para omitir las medidas de control.

- Disponibilidad de descifrado de SSL más rápido y escalable.
- Microsegmentación para descifrado selectivo sobre la base de contenido, dispositivos, usuarios o grupos.

Controles para aplicaciones en la nube y redes sociales para administrar de cerca a qué aplicaciones basadas en la nube y sitios de redes sociales se puede acceder y cuáles se pueden usar.

- Análisis avanzado de aplicaciones e inspección profunda de paquetes.
- Administración de contenido de aplicaciones de redes sociales, como Facebook, Twitter, LinkedIn y Pinterest.
- Control pormenorizado de aplicaciones evasivas en la nube, como TOR, BitTorrent, SnapChat, Skype y otras.
- Aplicación de Safe Search para Google, Bing y Yahoo.
- Búsqueda por imágenes segura y filtrado de traducciones para Google Services.

Protección de dispositivos móviles para ampliar la cobertura de la seguridad cibernética de todos los dispositivos móviles de una organización, independientemente de dónde o cuándo se utilicen.

- Filtrado de contenido completo para todos los dispositivos iOS, Android, Windows, Mac y Chromebook.
- Administración de políticas de Wi-Fi para invitados y de dispositivos propios de los usuarios.

Características principales *(continuación)*

Protección para navegadores y sistemas operativos desactualizados para que la protección de las tecnologías implementadas se pueda ampliar después del final de la vida útil, cuando los proveedores dejan de emitir actualizaciones de seguridad y parches para estas tecnologías.

- Protección para el final de la vida útil del navegador.
- Protección para el final de la vida útil del sistema operativo.

Informes avanzados en tiempo real para optimizar el proceso de producción de informes oportunos, precisos y profesionales para un rango de fines de cumplimiento y de administración interna.

- Informes exhaustivos y detallados.
- Informes en directo, informes de historiales e informes de estadísticas.
- Programación y personalización de informes.
- Búsqueda de eventos, que incluye la identificación y el bloqueo del uso de protocolos evasivos.
- Activación automática de grabación de video de escritorios (DMCR).
- Integración nativa con Splunk e integración con SIEM para informes forenses.

Administración desde un único panel permite a los sistemas escolares establecer y aplicar políticas de seguridad cibernética en todo el distrito mediante la nube, con flexibilidad para delegar algunas decisiones de la política a escuelas individuales.

- Consola de administración en la nube con interfaz de usuario web con capacidad de respuesta.
- Administración completa de políticas bidireccionales.
- Integración de directorios y administración de grupos sencillas.
- Administradores delegados del sistema y grupos de generación de informes.
- Políticas basadas en ubicaciones.
- Marca personalizada en las páginas de inicio de sesión y de bloqueo del usuario final.

Supervisión y ajuste del ancho de banda para dar visibilidad a los sistemas escolares en cuanto a la utilización del ancho de banda, con el fin de garantizar la disponibilidad mediante la detección de problemas y la reducción del uso indebido.

- Configuración y supervisión centralizadas de políticas/umbrales para reducir el uso indebido del ancho de banda.
- Garantía de la disponibilidad del ancho de banda en momentos y lugares críticos, por ejemplo, cuando se administran pruebas adaptativas/estatales mediante los dispositivos de los alumnos en el aula.

Soporte técnico de alta calidad, con técnicos de iboss altamente capacitados y experimentados para ayudar a los clientes con cualquier problema técnico o pregunta que puedan tener. Existe una variedad de ofertas de servicios disponibles para satisfacer las necesidades de los clientes de educación preescolar, primaria y secundaria.

Acerca de iboss

La plataforma Distributed Gateway Platform de iboss es un servicio de puerta de enlace web diseñado específicamente para resolver los desafíos que presenta la protección de las organizaciones distribuidas. El servicio de iboss fue creado para la nube y aprovecha una arquitectura revolucionaria basada en nodos que se amplía fácilmente para satisfacer las crecientes necesidades de ancho de banda y se administra a través de una única interfaz. La plataforma Distributed Gateway Platform de iboss está respaldada por más de 110 patentes y protege a más de 4000 organizaciones de todo el mundo. Esto convierte a iboss en una de las empresas de seguridad cibernética de más rápido crecimiento del mundo.

Para obtener más información, visite www.iboss.com o comuníquese con iboss escribiendo a sales@iboss.com.

Vea a iboss en acción. Solicite una demostración.