Hoja de datos

Data Loss Prevention

Riesgos de seguridad para las organizaciones distribuidas

Las infracciones de datos son más comunes que nunca, lo que aumenta la necesidad de que las empresas supervisen y controlen las comunicaciones de la red para evitar fugas y pérdida de información confidencial. Con oficinas remotas y empleados que trabajan desde dispositivos móviles, las organizaciones distribuidas de hoy en día están expuestas a un riesgo constante de pérdida de datos confidenciales. La plataforma Distributed Gateway Platform de iboss brinda seguridad de red completa que se puede administrar desde una consola central en tiempo real.

El conjunto de características de prevención de pérdida de datos (DLP, Data Loss Prevention) ofrece capacidades integrales de prevención de pérdida de datos basadas en archivos que detectan y detienen la transferencia de datos confidenciales hacia y desde la nube, al mismo tiempo que mantienen informados a los equipos de seguridad mediante alertas automáticas. Esto proporciona protección contra el uso no autorizado de la nube y protección contra pérdida de datos confidenciales para el uso de la nube, lo cual garantiza que los datos confidenciales estarán protegidos y se mantendrán dentro de los servicios en la nube aprobados por la organización.

Características principales

- Motores de detección y análisis de contenido incorporados
- Análisis profundo de archivos comprimidos
- Análisis de contenido dirigido
- Protección de pérdida de datos sencilla para todos los usuarios, las ubicaciones y los dispositivos
- Visibilidad en tiempo real para la aplicación de cumplimiento
- Plataforma única para administración y generación de informes

Distributed Gateway Platform de iboss Arquitectura única basada en nodos

La plataforma Distributed Gateway Platform de iboss está diseñada específicamente para satisfacer las necesidades de seguridad cibernética de las organizaciones distribuidas, pero lo hace de una manera completamente diferente. La plataforma Distributed Gateway Platform de iboss fue creada para la nube y puede defender las redes complejas y descentralizadas de hoy en día, así como las sucursales, las ubicaciones remotas y los usuarios móviles que dependen de ellas. La plataforma Distributed Gateway Platform de iboss también brinda la flexibilidad necesaria para instalar y reemplazar sistemas existentes en las instalaciones, lo que permite a las organizaciones realizar la transición a la nube sin inconvenientes, a su propio ritmo y sin la necesidad de volver a diseñar la arquitectura de las redes existentes.

Características principales

Motores de detección y análisis de contenido incorporados

Con una configuración mínima, los motores de detección avanzada seleccionan el contenido para evitar la pérdida no deseada de información confidencial, incluida la información de identificación personal, los números de tarjetas de crédito y los datos de bandas, junto con otros tipos diversos de contenido. Los motores de análisis de contenido procesan y analizan los archivos dirigidos, asegurando que incluso el contenido comprimido sea accesible para los motores de detección, que luego realizan una inspección en busca de información confidencial, emiten alertas y detienen las transacciones de datos según sea necesario.

Los motores avanzados de detección de contenido pueden identificar la siguiente información dentro de los datos:

- Números de tarjeta de crédito
- Información de identificación personal (PII)
- Direcciones de correo electrónico
- Datos de mapas GPS
- Claves de cifrado AES
- Datos de bandas de tarjetas de crédito
- Números de teléfono
- Datos de mapas KML
- Directorios de Windows

Los motores avanzados de análisis de contenido pueden inspeccionar los siguientes tipos de archivos:

- Base16
- GZip
- PDF
- Archivos de datos de Outlook
- Base de datos SQLLite
- Ejecutables de Windows PE
- Archivos ZIP
- Archivos RAR
- Archivos de hibernación de Windows
- Archivos LNK de Windows
- Archivos de Windows PE

Análisis profundo de archivos comprimidos

El control pormenorizado sobre la profundidad del análisis permite realizar búsquedas de contenido profundas dentro de los archivos comprimidos. La configuración de DLP especifica cuántos niveles se atravesarán cuando se analicen archivos zip que se encuentran dentro de archivos zip. Los ataques de denegación de servicio utilizan estos archivos zip anidados que, cuando los abre un destinatario inadvertido, pueden consumir grandes cantidades de tiempo y recursos del sistema y dejar la seguridad de una red sobrecargada y propensa al incumplimiento.

Análisis de contenido dirigido

Faculte a los administradores de seguridad de la red para crear reglas personalizadas que determinen cómo se aplican las políticas de DLP a su organización. Los administradores pueden configurar estas reglas para evaluar de manera selectiva los archivos en función del tipo de contenido, los métodos de solicitud, los destinos y los patrones de búsqueda, lo que aumenta la especificidad. La ejecución secuencial de las reglas priorizadas garantiza la aplicación de las políticas apropiadas para los usuarios de todos los niveles de permisos. Cuando el tráfico de archivos de alto riesgo alcanza los umbrales de actividad predeterminados, se activan las alertas automáticas y las acciones de seguridad para informar a los administradores y evitar la pérdida de datos.

Protección de todos los usuarios, las ubicaciones y los dispositivos contra la pérdida de datos

La aplicación de la política de seguridad en todos los usuarios, las ubicaciones y los dispositivos a través de una única plataforma garantiza la protección contra la pérdida de datos, incluso cuando los empleados trabajan de forma remota. Al aprovechar una arquitectura flexible basada en nodos, la plataforma Distributed Gateway Platform de iboss ofrece DLP, que se puede configurar en horas, no en días, sin la necesidad de una nueva arquitectura de red.

Visibilidad en tiempo real para aplicación de cumplimiento en todas las IP conectadas

Al aprovechar una arquitectura basada en nodos, las organizaciones grandes y distribuidas pueden aplicar globalmente políticas de seguridad que cumplan con la regulación en todos los usuarios y dispositivos, de acuerdo con las regulaciones de datos de información de identificación personal y de información de salud de los pacientes requeridas por la HIPAA, PCI y otras leyes federales. Además, la generación de informes centralizada en sitios o en usuarios y dispositivos individuales se realiza en cuestión de segundos, lo cual reduce los gastos generales de administración.

Plataforma única para administrar políticas y ver informes en tiempo real en todos los dispositivos y usuarios, en cualquier lugar

La plataforma Distributed Gateway Platform de iboss proporciona una única consola de administración basada en la nube para administrar políticas y ver la actividad del usuario y del dispositivo en tiempo real. Esto elimina la necesidad de administrar una consola "híbrida", que recibe o envía informes desde y hacia múltiples plataformas. Los informes detallados permiten a los administradores configurar políticas e informes para cumplir con las regulaciones locales en segundos.

¿Desea obtener más información? Solicite una demostración.

Acerca de iboss

iboss ha creado la primera y única plataforma de puerta de enlace distribuida que está específicamente diseñada para resolver el desafío de protección de las organizaciones distribuidas. El servicio de iboss fue creado para la nube y aprovecha una arquitectura flexible basada en nodos que proporciona seguridad avanzada para las organizaciones y las escalas descentralizadas de hoy en día para satisfacer las necesidades de ancho de banda cada vez mayores que se presentarán en el futuro. La plataforma Distributed Gateway Platform de iboss está respaldada por más de 100 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.

iboss, Inc. • U.S. HQ 101 Federal Street, 23rd Floor, Boston, MA 02110