Defensa avanzada contra amenazas (ATD) En la nube

Funciones FireSphere patentadas que acaban con las infecciones evasivas para reducir la pérdida de datos

El crecimiento de la computación en la nube en combinación con el desafío que supone proteger su empresa de las APT, amenazas evasivas y pérdidas de datos de hoy en día, convierten la defensa avanzada contra amenazas en un objetivo principal en cualquier sector. Tal y como ilustran numerosas violaciones de seguridad de alto perfil, acabar con el 100 % del malware es imposible. Sin embargo, aunque la mayoría de soluciones de seguridad basadas en la nube aseguran poder proporcionar protección frente a las APT, lo hacen únicamente a través de sedes corporativas. No pueden abarcar usuarios remotos y móviles sin un retroceso de datos y sin crear latencia, ni dejar a los usuarios móviles desprotegidos. Solo la Defensa contra APT FireSphere™ de iboss proporciona funciones ATD directamente a la nube, ofreciendo seguridad a todos sus usuarios de roaming y remotos sin la necesidad de datos de retroceso. La Defensa avanzada contra amenazas de iboss Cloud no requiere ningún tipo de hardware o software para implantarse y mantenerse, reduce los costes generales e incrementa la protección frente a pérdidas de datos y amenazas avanzadas.

Las ventajas de iboss

Proporciona defensa avanzada contra amenazas a través de toda su empresa, en cualquier lugar, en cualquier momento y en cualquier dispositivo

- ✔ Incluye zona de pruebas de comportamiento para detectar y detener el malware polimórfico antes de que penetre en el perímetro de su red
- ✔ Combina una incomparable detección de infecciones y defensa contra malware sin firmas a través de todos los sitios y usuarios en cuestión de minutos, sin datos de retroceso
- ✔ Ofrece flexibilidad con opciones en la nube públicas y privadas para empresas restringidas por cumplimiento normativo o que prefieren una solución local
- ✔ Utiliza fuentes en la nube sobre amenazas globales para proporcionar una detallada inteligencia forense y de investigación contra malware a través del exclusivo Centro de comandos de CISO y la Inteligencia de amenazas basada en la nube.
- ✔ Detecta malware previamente desconocido/no clasificado dentro de su red con monitorización patentada de anomalías de datos, incrementando la capacidad de su empresa para detectar las amenazas más maliciosas
- ✔ Reduce la pérdida de datos durante un ataque, y al mismo tiempo reduce el tiempo de respuesta ante un incidente con tecnología de contención y extracción de datos, proporcionando visibilidad a través de todos los vectores de amenazas
- ✔ Reduce el registro ruidoso de eventos consolidando los eventos en incidentes para datos de inteligencia más fiable, reduciendo los tiempos de respuesta ante un incidente con el Centro integrado de comandos de CISO.
- ✔ Escanea y asegura todos los puertos y protocolos, incrementando su capacidad para detectar y detener amenazas evasivas de puertos tales como ZeuS que hacen uso de la red TOR
- ✔ Ofrece más opciones para gestionar tráfico SSL que cualquier otra solución, aumentando la capacidad de su empresa para detectar amenazas en tráfico cifrado, incluyendo BYOD y wifi de invitados

La Defensa avanzada contra amenazas (ATD) de iboss asegura todas las ubicaciones y dispositivos en cuestión de minutos, sin datos de retroceso, disminuyendo el CAPEX/OPEX

- ✔ Asegure una gran empresa distribuida en cuestión de minutos sin necesidad de datos de retroceso
- ✔ Olvídese de dispositivos costosos que requieren muchos recursos, mantenimiento constante y actualizaciones regulares
- ✔ Amplíe o disminuya los servicios instantáneamente para ajustarse a cualquier requisito de la empresa; pague solo por los servicios que necesita
- ✔ Disminuya el coste total de propiedad (TCO) y conserve recursos TI, sin comprar, gestionar ni mantener ningún tipo de hardware o software
- ✔ Combine sus necesidades de control local con la flexibilidad y escalabilidad de una solución de Seguridad como Servicio con la opción Private Cloud de iboss

iboss CLOUD

La plataforma iboss Cloud se implementa instantáneamente para brindar tecnología de última generación patentada de iboss directamente a la nube, incluyendo nuestras exclusivas funciones avanzadas de defensa contra amenazas. iboss ofrece opciones públicas y privadas en la nube (Public Cloud y Private Cloud), para que pueda satisfacer las necesidades de su empresa con la máxima flexibilidad.

Public Cloud: El almacenamiento exclusivo le garantiza que sus datos jamás se mezclarán con otros datos de su empresa.

Private Cloud: Ofrece sensores locales para algunas funciones y, al mismo tiempo, envía oficinas remotas y usuarios de roaming directamente a la nube sin datos de retroceso ni tiempos de espera.

Descripción de funciones

Zona de pruebas de comportamiento distribuida

La Zona de pruebas de comportamiento de iboss analiza archivos sospechosos ejecutándolos en un entorno aislado y observando sus comportamientos. Utiliza una combinación de reglas y actividades de ensayo y error para determinar si un archivo representa o no una amenaza y proporciona información específica sobre los comportamientos y el contexto de dicha amenaza. Entre estas funciones se incluyen:

- ✔ Depósito automático de archivos sospechosos
- ✔ Implantación con múltiples instancias basada en la nube que permite un equilibro de carga automático para que se puedan ejecutar varias instancias en una sola red, sin latencia
- ✔ Configuración basada en el usuario que le permite configurar sus propias máquinas virtuales (VM) personalizadas y observar cómo se comporta un archivo en múltiples entornos, tales como WinXP, Win7, etc.
- ✔ Integración de reporte con la Consola de eventos y amenazas de iboss que ofrece análisis detallados y alertas instantáneas
- ✔ Depósito manual de cualquier archivo a la zona de pruebas para su análisis

Monitorización de anomalías en la red

FireSphere de iboss utiliza visibilidad total de flujo Web en todos los canales de datos entrantes/salientes para controlar continuamente el tráfico, detectar anomalías y detener la transferencia de datos sospechosos para reducir la pérdida de datos. Entre estas funciones se incluyen:

- ✔ Visibilidad total de flujo Web e indexado dinámico para acceder a registros de datos históricos y crear puntos de referencia para un tráfico normal
- ✔ Control continuo a través de una amplia gama de parámetros, incluyendo cómputos de conexiones, destino, bytes de entrada/salida y desviaciones de tráfico para detectar comportamientos inusuales que podrían significar que la red está en peligro
- ✔ Contención automática de transferencias de datos y alertas cuando surge un problema, dándole tiempo para investigarlo y remediarlo antes de que se produzca la pérdida de datos

Centro de comandos de CISO

FireSphere elimina ruidos y falsos positivos con alertas priorizadas, indicando qué máquinas necesitan una solución y porqué. Entre estas funciones se incluyen:

- ✔ Relaciona información de alertas con el nombre de usuario/máquina del directorio, junto con una imagen de activaciones históricas globales
- ✔ Elimina ruidos y falsos positivos con un profundo análisis forense en tiempo real
- ✔ Prioriza la severidad de amenazas añadiendo datos desde millones de motores de malware líderes y terminales globales
- ✔ Detecta malware evasivo que ya se encuentra en la red controlando y mapeando alertas de infecciones
- ✔ Inocula contra futuros ataques identificando nombres de IP y archivos alojados maliciosos

Nube de inteligencia contra amenazas

La Nube de inteligencia contra amenazas analiza cómo está actuando una amenaza en en general y qué patrones está mostrando, lo que puede predecir un comportamiento futuro y proporcionarle el contexto completo que necesita para remediar rápidamente problemas sin tener que lidiar con los ruidos y falsos positivos que generan otras soluciones.

Para más información:

Ficha técnica de la Plataforma iboss Cloud

Ficha técnica de la Plataforma pasarela de seguridad Web

Acerca de la ciberseguridad de iboss

La ciberseguridad de iboss protege las complejas redes distribuidas de hoy en día de las APT y amenazas específicas que ocasionan la pérdida de datos con la Plataforma pasarela de seguridad Web de última generación de iboss, haciendo uso de una innovadora arquitectura en la nube y avanzadas tecnologías patentadas de defensa contra amenazas. Para más información, visite nuestro sitio web: **www.iboss.com.**

DS/ATDC-01/16

iboss, Inc. · 877.742.6832 · sales@iboss.com · U.S. HQ 4110 Campus Point Court · San Diego, CA 92121